LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multimethodology Research

Kämppi, Pasi

2011 Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multimethodology Research

Pasi Kämppi
Information Systems
Thesis
May, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Ylempi ammattikorkeakoulututkinto
Tietojärjestelmäosaamisen koulutusohjelma

Pasi Kämppi

Monimenetelmällinen tutkimus satelliittipaikannukseen perustuvien järjestelmien teknisistä riskeistä

Year 2011 Pages 46

Satelliittipaikannus ja siihen perustuvat sovellukset ovat kasvava liiketoiminnan alue ympäri maailmaa. Paikannuslaitteet ovat edullisia, mobiiliverkkojen peitto on kasvanut ja internetistä on tullut osa jokapäiväistä elämäämme. Tämä kehitys on mahdollistanut myös satelliittipaikannuksen hyödyntämisen useissa sovelluksissa.

Satelliittipaikannusta käytetään monissa liiketoimintakriittisissä sovelluksissa kuten kuljetuskaluston ja arvokuljetusten seurannassa. Sovellusten yhteydessä mainostetaan vain niitten tuomia hyötyjä, mutta mahdollisista riskeistä ei ole mainintaa. Laureassa tehtiin aloite Saterisk-projektille, joka tutkii satelliittipaikannuksen lainopillisuuteen, käytettävyyteen ja tekniikkaan liittyviä riskejä. Projekti sai rahoituksen TEKES:lta ja projekti alkoi elokuussa vuonna 2008. Projektin päävastuu on Laurealla ja projektin yhteistyökumppaneina ovat myös Lapin Yliopisto ja toimijoita yksityiseltä sektorilta.

Tämän tutkimuksen päätavoite oli kartoittaa satelliittipaikannukseen ja sitä hyödyntaviin sovelluksiin liittyviä teknisiä riskejä. Toissijainen avoite oli tuottaa kansainvälisesti tunnustettua tutkimustyötä ja siihen liittyviä julkaisuja. Tämä raportti ei käsittele lainopillisuuteen tai käytettävyyteen liityviä riskejä.

Tutkimuksen aikana käytettiin monimetelmällistä suunnittelututkimusta. Monimenetelmällinen suunnittelututkimus esittää kuinka teorian kehittäminen, tutkimusmenetelmät, kokeellisuus ja järjestelmäkehitys muodostavat yhtenäisen tutkimusprosessin. Tutkimusta arvioitiin suunnittelututkimuksen seitsemän ohjesäännön perusteella. Tutkimusprosessin aikana käytettiin useita tutkimusmenetelmiä kuten kvalitatiivista riskianalyysia, grounded teoriaa, simulaatiota ja kenttätestausta.

Tämä raportti esittää neljän kansainvälisen julkaisun tulokset vuosilta 2009 ja 2010. Ensimmäinen ja toinen julkaisu käsittelevät satelliittipaikannusjärjestelmiin liittyviä tietoturvariskejä. Järjestelmä on monimutkainen ja on altis useille haavoittuvuuksille. Kolmas julkaisu esittelee satelliittipaikannusjärjestelmille räätälöidyn riskianalyysimenetelmän, järjestelmään liittyviä teknisiä riskejä ja tulokset kolmesta riskianalyysisimulaatiosta. Simulaatioiden perusteella todettiin, että riskiprofiilit ovat riippuvaisia käyttäjän vaatimuksista ja sovelluksen ominaisuuksista. Neljäs ja viimeinen julkaisu keskittyy käytännön testaukseen oikealla satelliipaikannusjärjestelmällä ja siinä esitetään myös mittaustulokset tiedonsiirron luotettavuudelle ja paikannustarkkuudelle.

Avainsanat: kenttätestaus, riskianalyysi, satelliittipaikannus, tietoturva

Laurea University of Applied Sciences **Abstract**
Leppävaara
Master of Business Administration
Information Systems

Pasi Kämppi

Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multimethodology Research

Year 2011 Pages 46

Satellite-based tracking is a rapidly growing business area in many parts of the world. Tracking devices have become inexpensive, mobile network coverage has grown, and the internet has become a part of our everyday life. This evolution has enabled the proliferation of satellite-based tracking applications.

Satellite based tracking is used with many business critical applications like fleet management or the tracking of cash in transit. Very often only the benefits of the satellite based tracking solutions are advertised while the risks and weak points are forgotten. A proposal was made for the Saterisk project to investigate legal, usability and technical risks in satellite based tracking. The project got funding from the Finnish Funding Agency for Technology and Innovation (TEKES) and began in 2008. The Saterisk project is headed by the Laurea University of Applied Sciences and it is made in cooperation with the University of Lapland and partners in private sector.

The primary objective of this research was to find the most significant technical risks for satellite based tracking systems and the emphasis was on ICT. The secondary objective was to generate internationally recognized R&D research work and publications. This report does not examine legal or usability issues for satellite based tracking systems.

This research work followed the multimethodological approach for IS research. In the multimethodological approach theory building, observation, experimentation and systems-developing phases are integrated during the research process. The research work was evaluated according to seven guidelines for IS design research. The framework also encourages the researcher to use several research and evaluation methodologies. During the research process several research and evaluation methodologies were used such as qualitative risk analysis, grounded theory, simulation and field testing.

This research report contains four international publications that were published during the years 2009 and 2010. The first and second publications cover information security related issues for satellite based tracking systems. The system is complex and it is vulnerable to many threats. The third publication presented a technical risk analysis procedure, with a list of possible technical risks and the results of three simulated risk analysis cases. It was found that the risk profiles are very dependent on use cases. The last publication investigates how the satellite based tracking system performs in real life and presents measured metrics for reliability and accuracy.

This report concludes the research work and presents a description of the satellite based tracking system, describes research methodologies and summarizes all publications.

Keywords: field testing, information security, risk analysis, satellite based tracking

Preface

It has been a great opportunity for me to work on the Saterisk research project. The project has given me the possibility to acquire new information and apply my existing knowledge in a new context, in addition I have benefited through personal growth and development.

I would like to thank the personnel of the Laurea University of Applied Sciences.

Dr. Jyri Rajamäki, who acted as supervisor for this thesis, encouraged me to write international publications and present them at international conferences. It was a great challenge for me and Dr. Rajamäki guided me with the practical issues. He also took part in the research project.

Robert Guinness (M.Sc), who is working on the Saterisk project, made a great contribution during the research project. He reviewed the publications and offered his help with many other issues too. He also acted as co writer in all publications.

Students had the opportunity to take part in the research process too. Tatu Urpila, a student of the degree programme in security management, acted as reviewer for two publications and as a co writer in one publication.

The management assistant of Laurea, Elina Pohja, helped me with the practical issues when I was preparing for the conferences. She booked flights and reserved accommodation.

My employer also supported me during the research and study process. I was allowed to take part in conferences and lessons that were arranged during office hours.

I got the greatest support from my family. My wife, Jenni, took care of the family business when I was at the conferences or when I had to write. My daughter, Pilvi, reminded me about her existence too. When she had a good day I was her best friend. On bad days she told me to go to my working room and do my job!

Espoo, May 2011

Pasi Kämppi

Table of Contents

List of Publications

P[1] P. Kämppi, J. Rajamäki, R. Guinness, Information security in satellite tracking systems, 3rd International Conference on Communication and Information Technology, Athens, Greece, Dec 2009, ISBN: 978-960-474-146-5, pp. 153-157.

P[2] P. Kämppi, J. Rajamäki, R. Guinness, Information security risks for satellite tracking systems, International Journal of Computers and Communications, Issue 1, Volume 3, 2009, ISBN: 978-5-900780-69-6, pp. 9-16.

P[3] P. Kämppi, R. Guinness, Technical Risk Analysis for Satellite Based Tracking Systems, Integrated Communications Navigation and Surveillance Conference, Herndon, VA, USA, May 2010, ISBN: 978-1-4244-7457-8, pp. M3-1 – M3-16.

P[4] P. Kämppi, R. Guinness, T. Urpila, Field Testing for Satellite Based Tracking Systems, 61st International Astronautical Congress, Prague, Czech Republic, Sep 2010, CD-ROM, 15 pages.

List of Abbreviations & Symbols

Android	Mobile operating system by Google
API	Application Programming Interface
Compass	Chinese satellite navigation system
CSNPAC	China Satellite Navigation Project Center
DoD	Department of Defense
EC	European Commission
ESA	European Space Agency
Galileo	Joint European satellite navigation system
Glonass	Global'naya Navigatsionnaya Sputnikowaya Sistema, Russian satellite based navigation system
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GPRS	General Packet Radio System
HDOP	Horizontal Dilution of Precision
HW	Hardware
ICT	Information and Communication Technologies
Internet	Global system of interconnected computer networks
iOS	Mobile operating system by Apple
IS	Information Systems
IT	Information Technology
LTE	Long Term Evolution
NAVSTAR	Former name of GPS
NMEA	National Marine Electronics Association
OBU	On Board Unit
SA	Selective availability
Saterisk	Research project that analyzes technical, legal and user related risks in satellite based navigation
SMS	Short Messages Service
SW	Software
Symbian	Mobile operation system by Symbian foundation
TEKES	Finnish Funding Agency for Technology and Innovation
TETRA	Terrestial Trunked Radio
TIMATION	Research project by Naval Research Laboratory
TRANSIT	Satellite navigation system for US submarines before GPS
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access

1 Introduction

Satellite-based tracking is a rapidly growing business area in many parts of the world. Tracking devices have become inexpensive, mobile network coverage has grown, and the internet has become part of our everyday life. This evolution has enabled the proliferation of satellite-based tracking applications.

Satellite based tracking is used with many business critical applications like fleet management or the tracking of cash in transit. Very often only the benefits of the satellite based tracking solutions are advertised while the risks and weak points are forgotten. A proposal was made for the Saterisk project to investigate legal, usability and technical risks in satellite based tracking. The project got funding from the Finnish Funding Agency for Technology and Innovation (TEKES) and began in 2008. The Saterisk project is headed by the Laurea University of Applied Sciences and it is made in cooperation with the University of Lapland and partners in private sector.

The Saterisk project has already produced many international publications and theses. The first thesis was written by Jouni Viitanen who was one of the Saterisk project originators. His thesis defined the requirements of the Saterisk project and it offered guidelines for future research work (Viitanen 2009). Markus Happonen continued the research work and he published his thesis in 2010. Happonen presented both intentional and unintentional interference scenarios in satellite based tracking. Happonen also handled the communication of the time critical data transfer between multinational organizations. (Happonen 2010.) The latest thesis work was published by Pertti Kokkonen. He considered the legality of tracking personal property if it is given to somebody else. He investigated some technical issues too. (Kokkonen 2010.)

Every one of the publications investigated possible risks in the selected research domains. However, none have provided system-level analysis of technical risk scenarios or presented a detailed system-level description for satellite based tracking system.

The primary objective of this research was to find the most significant technical risks for satellite based tracking systems and the emphasis was on ICT. Previous publications did not contain general technical description of the satellite based tracking system and it was defined during research work too. This report does not handle legal or usability issues for satellite based tracking systems. Legal issues were investigated by the University of Lapland.

The secondary objective was to generate internationally recognized R&D research work and publications. This objective meets the strategic goals of the Laurea University of Applied Sciences.

This research followed the multimethodological approach for IS research. In the multimethodological approach theory building, observation, experimentation and systems developing phases are integrated during the research process (Nunamaker, Chen & Purdin 1991). The main objective of this research process was to analyze and evaluate a satellite based tracking system, not to develop the system itself. Nevertheless, analysis tools and a real testing environment were developed and integrated in the observation and experimentation phases. The analysis tools combined many research methodologies such as qualitative risk analysis, grounded theory and simulation. Experiments were made with the real satellite based tracking system.

This research was evaluated using the framework for IS design research. The framework gives seven guidelines for researchers how to construct, present and evaluate their research work. The framework also encourages the researcher to use several research and evaluation methodologies. Readers can use the framework for understanding IS design research. (Hevner, March, Park & Ram 2004.)

This research report contains four international publications that were published during the years 2009 and 2010. The first and second publications covers information security related issues for satellite based tracking systems. The system is complex and it is vulnerable to many threats. The third publication presented a technical risk analysis procedure, with a list of possible technical risks and the results of three simulated risk analysis cases. It was found that the risk profiles are very dependent on use cases. The last publication investigates how the satellite based tracking system performs in real life and presents measured metrics for reliability and accuracy.

The next chapter gives basic information about the history of satellite based navigation, presents the principle of satellite based tracking system and introduces four applications for satellite based tracking. The third chapter presents the methodologies that were used during the research process. In the fourth chapter all publications are summarized and the fifth chapter concludes the research work.

2 Satellite based tracking

2.1 History of satellite based navigation

The history of modern satellite navigation started in December 1973 when the Department of Defense (DoD) approved the Global Position System/NAVSTAR project. The target of the project was to combine the best practices of existing navigation projects 621B, TRANSIT and TIMATION. The existing projects were headed by the US Air Force or the Navy and they were competing with each other. The new navigation system was decided to be only for military use. (Stanford University News Service 1995.)

The first Global Position System (GPS) satellite was launched in February 1978 and the constellation of the 24 satellites was achieved on 1988. In 1983 civilians were allowed to use GPS. The reason being that a Korean airplane had got lost over Soviet borders and been shot down. However, the accuracy of the civilian signal was limited by the selective availability (SA). GPS was allowed for global use free of charge in 1993 and SA was disabled on 2000. (kowoma.de 2009, History of NAVSTAR GPS.)

2.2 Principle of satellite based navigation

This chapter presents the basic principle of satellite based navigation. Information is based on GPS satellite navigation system but the principle is the same with other satellite based navigation systems too.

Satellite based navigation is based on signals that are delivered by the satellites. The satellites orbit the earth at a height of 20200 km at a speed of 3.9 km per second. The orbit time is 12 hours. (kowoma.de 2009, GPS Satellite Orbits.) The satellites are powered by solar panels and the signal transmission power is about 50 watts. The estimated life time of the satellites is 4.5 – 7.5 years depending on the satellite model. (kowoma.de 2009, GPS Satellites.) Figure 1 presents satellites in their orbits.

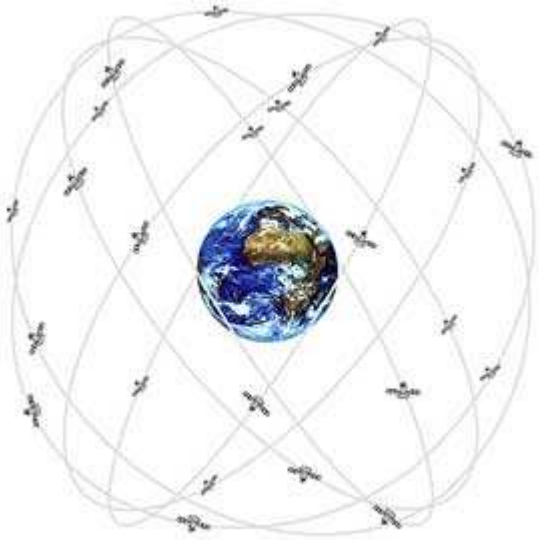


Figure 1 GPS satellites in their orbits (kowoma.de 2009, GPS Satellite Orbits)

The satellites deliver a signal that contains satellite identification, satellite position and the time when the signal was delivered. A GPS receiver compares the signal timestamp with the time when the signal was received and calculates the distance between receiver and satellite. The distance calculation is based on time difference between the sending and receiving time. (kowoma.de 2009, Position Determination with GPS.)

When the GPS receiver knows the distance to the three satellites the position information is calculated by triangulation. A two dimensional position fix (2D), that includes latitude and longitude, requires signals from three satellites. The 2Dfix does not include altitude information. A three dimensional position fix (3D) with the altitude can be calculated when the signal from four satellites is available. (kowoma.de 2009, Position Determination with GPS.) The principle of calculation of the 2D position fix is presented in Figure 2.

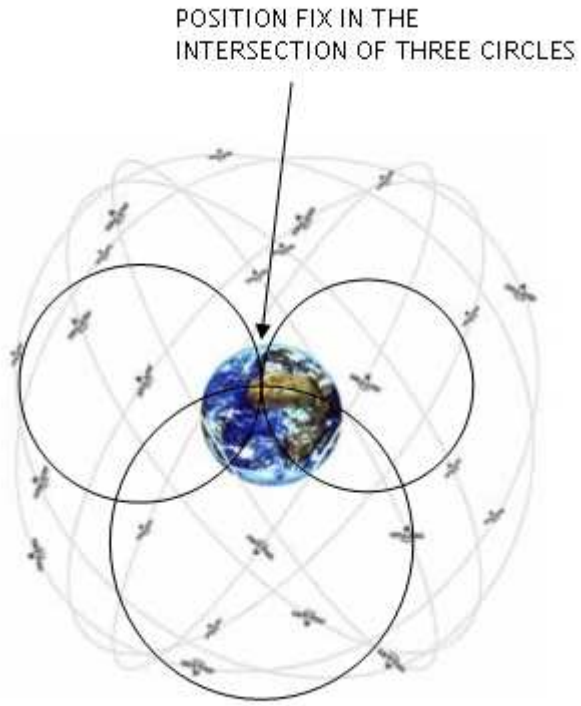


Figure 2 Principle of calculation 2D position fix

2.3 Technical system description for satellite based tracking

A modern satellite-based tracking system combines navigation and telecommunications technologies. The system is complicated and it consists of many technical segments, including the control segment, space segment, tracking segment, communication segment, data processing segment, application interface for external applications and end-user segment. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS), and positioning data is delivered for post-processing via mobile networks, the internet or a secure network. (Kämppi, Guinness and Urpila 2010.) The principle is illustrated in figure 3.

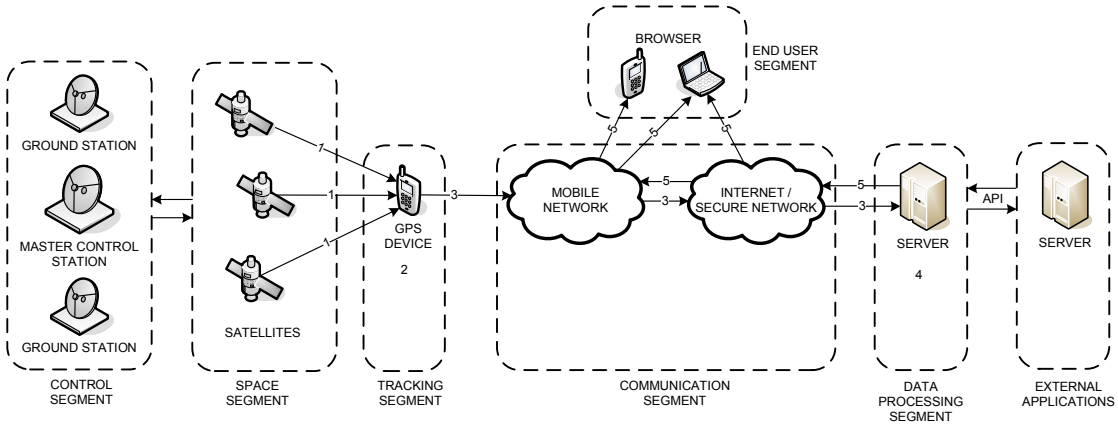


Figure 3 Principle of a satellite based tracking system (Kämppi at al 2010)

The sequence of the tracking:

1. Signals are delivered by the satellites
2. GPS receiver calculates the position
3. Position data is sent for post processing
4. Position data is processed and stored
5. End user access to position data

The following sections describe the segments of the system more deeply.

2.3.1 Control segment

The control segment contains the master control station and the ground stations that monitor satellites in the space segment. Monitoring is made 24 hours in day. Ground stations receive monitoring data from satellites and they forward data to the master control station. The master control station analyses monitoring data and sends adjustment commands to the satellites via the ground stations. (kowoma.de, Control Segment.)

2.3.2 Space segment

The space segment contains systems to deliver signals for calculating position.

GPS (Global Positioning System) is the most commonly used satellite positioning system at the moment. Even though the GPS system is developed and operated by the United States Air Force for the Department of Defence, it is available for civilian use all over the world as well. The system currently contains 31 active satellites and it covers almost the entire world. (InsideGNSS, About GPS.) Replacing old satellites has experienced some delays, but the new generation of satellites now being sent to into orbit will be carrying new technology to ensure reliability (U.S. Air Force 2010). The position determined by the GPS system is accurate to

about 10-20m, since the U.S. government stopped intentionally degrading the signal for civilian use in 2000 (About.com 2000).

GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) was developed and is maintained by the Russian government. The system is similar to the GPS and it should be able to offer as good accuracy as the GPS system. Compatibility with other GNSS systems is possible and at the moment is being further developed. (InsideGNSS, About GLONASS.) The satellite constellation of the system has improved during the past few years and contains 21-23 active satellites at the moment (Russian Federal Space Agency, Information-Analytical Centre 2011).

Galileo is under development by the European Commission (EC) and the European Space Agency (ESA) (ESA 2010, Whos´s involved in Galileo). The overall objective of the Galileo program, however, is to develop an independent navigation service for civilian use with better performance than the current GPS service. Galileo is technically similar to GPS and GLONASS. (ESA 2010, Why Europe needs Galileo.) The full constellation will contain 30 satellites in the future (ESA 2010, What is Galileo).

Compass is under development by the China Satellite Navigation Project Center (CSNPC). China is planning to have a 12 satellite constellation, providing regional coverage and to the in operation in 2012. The full 35 satellites constellation is aimed to be complete in 2020 as the funding is already assured. (InsideGNSS, What is COMPASS.) The first satellite was launched in January 2010 and after the launch of the fifth satellite on August 1st 2010, the project is on course to complete its targets (National Aeronautics and Space Administration 2010).

2.3.3 Tracking segment

The tracking segment contains devices that are able to calculate and deliver position information for post processing. Today many mobile phones include GPS receivers, and it is easy to turn a mobile phone into a tracking device (Aspicore). For professional services and public authorities, TETRA clients and tracking-only clients (without communications functionality) are available (Motorola; Velocitybox). New positioning devices will support three systems (GPS, GLONASS, and Galileo) so that several techniques can be used simultaneously to guarantee better positioning accuracy and availability (GPSworld).

2.3.4 Communication segment

The communication segment contains systems to deliver positioning data for post-processing and use by end-users.

General Packet Radio System (GPRS) is an extension of the Global System for Mobile Communications (GSM), and it offers mobile packet-switched access. The data rate offered is 40-300 kbit/s, and the round trip time (RTT) is up to a few seconds. (3GPP, GPRS.) GSM offers connectivity in more than 218 countries and covers more than 80% of the world's population (GSM World, GSM).

Universal Mobile Telecommunications System (UMTS) is the successor to GSM. It offers voice, messaging and data services. (3GPP, UMTS.) The data rate is higher and the RTT is shorter compared to GSM. The data rate offered is up to 14 Mbit/s (3GPP, HSPA). Radio coverage is continually expanding, and UMTS covers the most populated areas.

Short Message Service (SMS) is the messaging service of GSM and UMTS. It allows users to send and receive text messages on a mobile phone. The length of messages is 160 characters, and messages can be sent globally via different operators. (3GPP 2009.)

Long Term Evolution (LTE) is fourth-generation (4G) telecommunication standard. LTE offers a packet-optimized service without native support for voice communication. The data rate offered is up to 300 Mbit/s with low RTT. (3GPP, LTE.) The first commercial networks were launched in Scandinavia in late 2009 (phone.com 2009).

Terrestrial Trunked Radio (TETRA) has been developed for professional services like police and fire departments (TETRA Mou Associaton, Markets & Applications). It offers voice, short data and packet data services. Strong security features and dedicated capacity are essential for professional use (TETRA Mou Associaton, Key Services). The latest release of TETRA offers data rates up to 500 kbit/s (TETRA Mou Associaton, Tetra Release 2).

Worldwide Interoperability for Microwave Access (WiMAX) is based on open 802.16 standards. WiMAX offers a packet-switched service, and voice communication is not supported. Data rates are up to 75 Mbit/s. (WiMax.com.) WiMAX is currently deployed in 149 countries, and 621 million people are covered (WIMAX Forum 2011).

2.3.5 Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data usable for end-users. End-users can access their services via the Internet or a secured network. Systems have to be connected to the Internet safely and reliably. Secured networks are used for the professional services. (Kämppi at al 2010.)

2.3.6 Application programming interface for external applications

API (Application Programming Interface) allows a software program to interact with other software and operating systems (PCMAG.COM). API makes it possible to combine the location data that we have acquired with other applications. Using API would also make it possible for us to do our own program that could use the data we have acquired and stored with the applications we have used. For example GpsGate service offers API so that users can send data to and receive data from the GpsGate-service to be processed with other applications. (GpsGate.com, Developer´s Guide GpsGate API.)

2.3.7 End user segment

The end-user segment offers customer interfaces for their positioning data. Typically the interface is offered via a network connection and web browser. Mobile terminals can be used as customer interfaces, too. (GpsGate, GpsGate Client.)

2.4 Applications for satellite based tracking

Satellite based tracking is used in many applications. The technological evolution of navigation and telecommunication equipment has enabled possibilities for many very interesting applications. From the researcher’s point of view, it is very important to know how satellite based tracking systems are used in real life. Sub segment sections present several applications and their special system requirements.

2.4.1 Fleet management

Fleet management is used to track cars, trucks, trailers and containers (SATCOM TECHNOLOGY, Fleet Management). The routes of trucks and trailers can be planned optimally to save fuel or vehicles can be directed to new routes in case of traffic accident. Fleet management can be integrated with geofencing and embedded car management functionality too. If the tracked vehicle, for e.g. a rent car, goes outside the allowed geographical area then an alarm

is triggered. With embedded functionality the ignition and brake system of a car can be managed remotely. (SATCOM TECHNOLOGY, Anti Hijack.)

Many commercial fleet management applications rely on commercial telecommunications networks. The quality of the networks can not be guaranteed and it is possible that the tracked vehicle will go outside the radio coverage or that the network is congested in highly populated areas. In an international environment roaming can cause problems. (Kämppi & Guinness, 2010.)

2.4.2 Traffic signal management

Traffic signal management is one of the most interesting applications for satellite based tracking. The Urban Traffic Control Centre of Helsinki has created a system called HeLMI that is able to create traffic signal priorities for busses and trams. Busses and trams are equipped with tracking devices that have integrated GPS and wireless modem functionality. The location data is sent is in real time to the central computer that calculates traffic signal priorities for busses and trams. (Urban Traffic Control Centre of Helsinki, Renewal of HeLMI.)

The system has a very strict requirement for data transfer reliability, deviation and delays. The data transfer delay and deviation has to be low because these metrics have a great effect on the system reliability. For example, if the signal from the bus is delayed on the data transfer path then the traffic signal priority is created too late. (Urban Traffic Control Centre of Helsinki, New Public Transportation Sensor.)

2.4.3 Cash in transit

The tracking of cash in transit is used to track the transportation of valuable goods. The tracked vehicle sends location data in real time to the tracking center and the location of the vehicle is monitored all the time. If the vehicle disappears or the vehicle departs from the preplanned route then it is a possible indication of a robbery or other threat. (TRACK24, ROADRUNNER.)

The cash in transit is one of the most demanding applications for satellite based tracking. It is possible that criminals will use jammers to interfere in real time tracking that they try to capture location data from telecommunications networks to find out used routes. The reliability of the system has to be on the highest standard to avoid false alarms.

2.4.4 Road toll

One of the latest applications for satellite based tracking is the road toll. The idea behind road toll is that tax is based on the type of vehicle, kilometers driven and routes. Cars are equipped with On Board Units (OBU). The OBU contains a GPS chip and a wireless modem and it is able to send taxing data in real time to the data center. If a car is outside of radio coverage the taxing data is buffered into the memory of the OBU. (The Slovak Spectator 2009).

The OBU has to work in a very demanding environment inside a car. The inside temperature and humidity of a car can vary a lot depending on the time of year. In other words, the OBU is under hard environmental stress during the year. The number of cars creates hard requirements for the whole tolling system. The system has to be able to handle a great number of tolling transactions with high reliability. Taxing data is not allowed to be lost in any circumstances. (Kämppi & Guinness 2010).

It is possible that the tolling system will be a potential target for hackers whose objective is to cause harm to the system or manipulate taxing data. It would be a great disaster if hackers were able to destroy taxing data for one month. (Kämppi, Rajamäki & Guinness 2009).

The latest possible threat to the road toll is the use of jammers. It is possible that some individuals are not willing to pay road toll and they would to use jammers to interfere with the OBU. (Kämppi & Guinness 2010). Jammers are very cheap and readily available via internet shops (JAMMER WORLD).

3 Research process description

3.1 Multimethodological approach

The objective of this research was to define the most remarkable technical risks for satellite based tracking systems. In practice we had to evaluate and analyze the different functionality aspects of satellite based tracking systems. In other words, we had to take the role of system developer although our objective was not to make improvements to satellite based tracking systems.

According to Nunamaker, Chen & Purdin “a research methodology consists of the combination of the process, methods, and tools that are used in conducting research in a research domain” (Nunamaker at al 1991.) In practice that means that a researcher has to be able to find suitable methods and tools for the research problem. It is quite obvious that broader research questions require the use of a wider range of methods and tools than narrower ones. Nuna-

maker at al also states that researchers may ask the wrong research questions if they do not have complete understanding of a research domain. (Nunamaker at al 1991).

Nunamaker at al present in their paper a multimethodological approach for IS research that integrates theory building, experimentation, observation and systems development phases together as in figure 4.

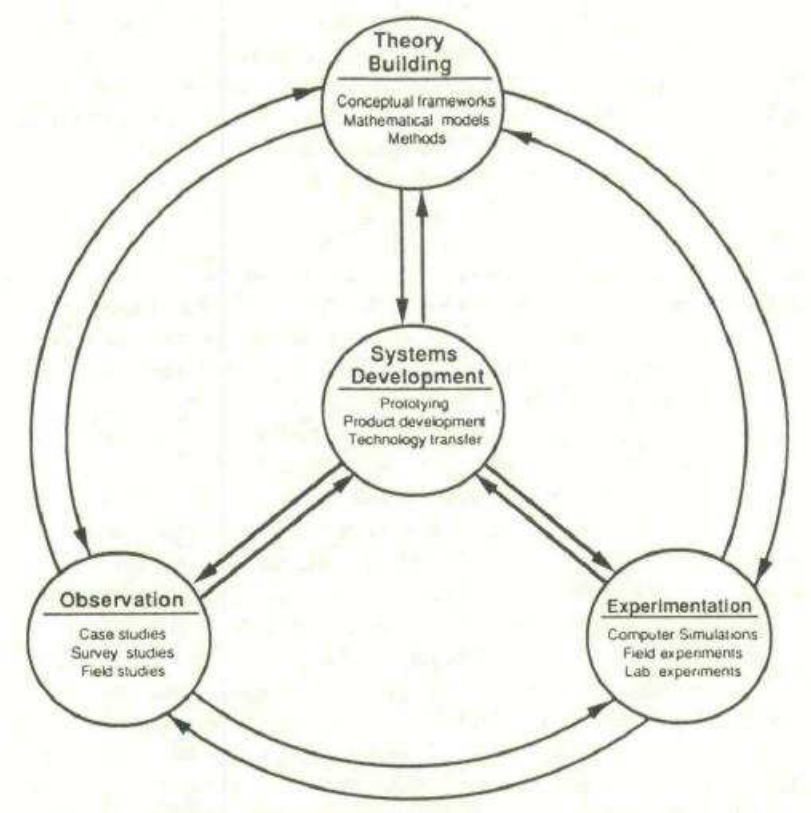


Figure 4 Multimethodological approach to IS framework (Nunamaker at al 1991)

Theory building provides basic knowledge for the research domain and it will raise new ideas, concepts, methods and models (Nunamaker at al 1991). This phase was included in every publication during the research process because every publication presented something new to the research domain. Before we started a new research phase (publication) we had to define the main objective for each publication. The theory building phase played a bigger role in the third publication [P3]. The third publication [P3] presented how qualitative risk analysis was integrated with grounded theory to find the most significant technical vulnerabilities for satellite based tracking systems. Grounded theory was used to categorize known technical vulnerabilities, form system segments and investigate relationships between the segments of the system. Qualitative risk analysis was used to define risk profiles for three use cases.

Observation is needed when is relatively little known about a research area and there is a need to get a general view of the research domain. Typical research methods at this phase are case studies, field studies and sample surveys. This phase may also provide ideas and guidelines for the experimentation. (Nunamaker at al 1991.) The observation phase was used in [P1], [P2] and [P3]. Publications [P1] and [P2] investigated information security in satellite based tracking systems by integrating existing knowledge in the new research domain. Generated information was reusable in [P3] and [P4]. The third publication [P3] continued to gain knowledge of the research domain and it combined together with more detailed technical information of telecommunications and satellite based navigation.

Experimentation is used when more practical knowledge is needed for the research domain. Laboratory and field experiments or computer and experimental simulations can be used. The results of experimentation may provide feedback to other research phases. (Nunamaker at al 1991.) The third publication [P3] presented the prototype of a risk analysis tool that was used to define risk profiles for three simulated use cases. The generated knowledge of [P3] was reused in [P4]. The idea of the last publication [P4] was to get real hands on experience of satellite based tracking by using a real satellite based tracking system and to define metrics for the data transfer reliability and position accuracy. The last publication [P4] also generated complementary knowledge for the previous research phases.

Systems development provides five stages for the research work: concept design, constructing the architecture of the system, prototyping, product development and technology transfer. This phase combines technological and theoretical knowledge into potential practical applications or prototypes. If the generated theories, concepts and systems are really useful they are transferred to organizations. (Nunamaker at al 1991.) As mentioned earlier the objective of this research was to analyze and evaluate satellite based tracking systems. Actual system development for satellite based tracking systems was not made during this research. Nevertheless, development work in other research phases was conducted. The prototype of a risk analysis tool that was used for simulation in the third publication [P3] required development work. Also the field testing setup in the last publication [P4] required system integration and development actions.

Figure 5 summarizes the multimethodological approach for this research.

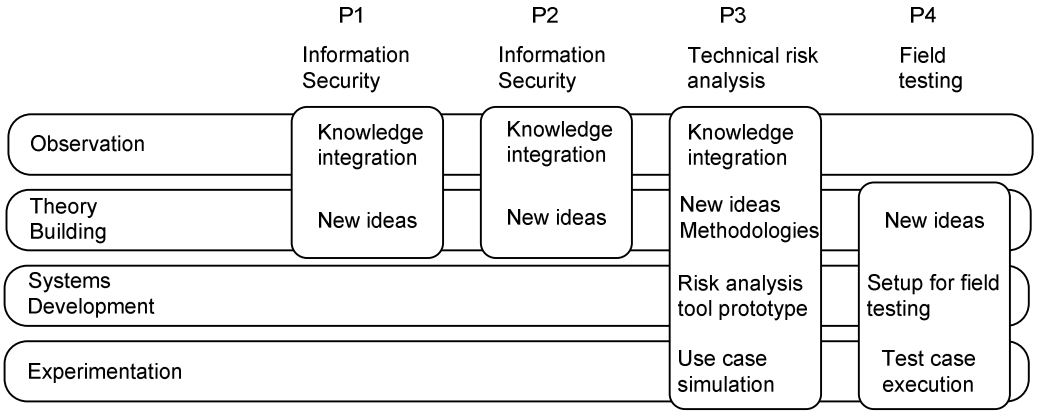


Figure 5 Multimethodological approach for research work

3.2 Research process evaluation

Hevner, March, Park & Ram (2004) present a research framework for IS design research. The purpose of the framework is to give guidelines for researchers how to conduct, evaluate and present their work. It also helps readers and editors to understand IS design research. (Hevner at al 2004.)

The design science is basically a problem solving paradigm. The target of IS design research is to solve identified problems and to create IT artifacts that meets the business needs. The IT artifact meets the target when it solves problems in an innovative way or improves current practices or solutions. (Hevner at al 2004.)

The problem space and business needs are defined by the environment (people, organizations, technologies). IS research solves the problems and creates artifacts that meet the business needs. IS research effectively uses the knowledge base that provides the foundational theories, frameworks, instruments, constructs, models, methods and instantiations used in IS research. When the problem is solved the artifact is added to the knowledge base. (Hevner at al 2004.)

The form of the artifact is not defined very strictly. The most important thing is that the artifact brings something new to the knowledge base. New IT artifacts can be defined as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems). The cycle of IS design research framework is presented in figure 6 (Hevner at al 2004.)

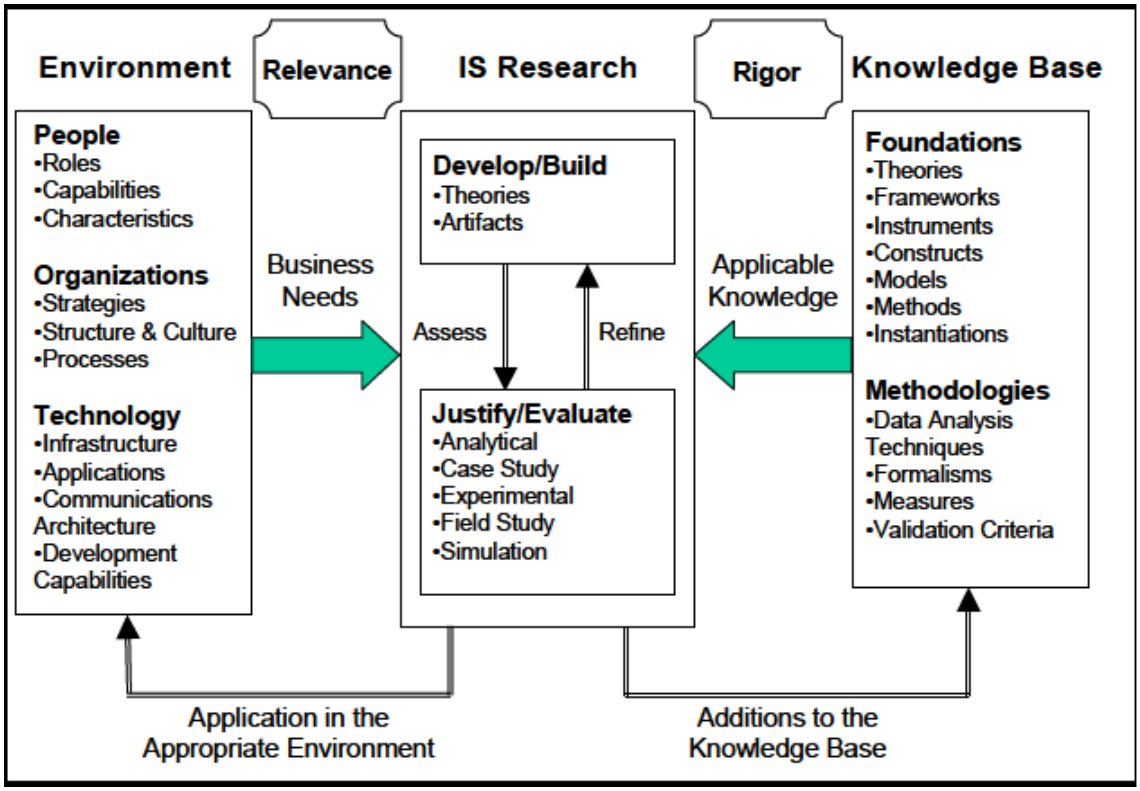


Figure 6 Research framework for IS design (Hevner at al 2004)

Hevner at al (2004) give seven guidelines for effective and rigorous design science research. The purpose of the guidelines is to assist researchers, reviewers, editors and readers to understand design science research. (Hevner at al 2004.) The following sections present the guidelines and explain how they were used during this research process.

Guideline 1 Design as an Artifact

The first guideline says that the artifact of design science research has to solve an identified problem. Research can generate several types of artifacts and the artifacts are rarely ready to be used in real life. The artifacts can be ideas, practices and technical capabilities. It is important that the information created by the artifact is reusable. (Hevner at al 2004.)

The problem space for this research was defined by the Saterisk project. The Saterisk project defines that the objective of this research is to find possible technical risks for the satellite based tracking system. The Saterisk project did not define the form of artifacts and researchers had full freedom to solve problems independently.

Guideline 2 Problem Relevance

The second guideline states that the objective of research is to create knowledge and understanding for future use. The research has to generate usable information for both IS researchers who plan, manage, and implement information systems and for IS researchers who plan, manage and implement technologies that are used in their development and implementation. (Hevner at al 2004.)

This research process created four international publications in 2009 and 2010. The acceptance processes for the abstracts and the publications ensured that the content of the publications is scientifically relevant and reusable. The first publication [P1] is already used as a reference in one publication (Viitanen, Happonen, Patama & Rajamäki 2009) and one master's thesis (Kokkonen 2010) and that shows the reusability of created information.

Guideline 3 Design Evaluation

The third guideline says that the utility, quality and efficiency of a design artifact must be rigorously demonstrated via proper evaluation methods. IT artifacts can be evaluated in terms of functionality, completeness, performance, reliability and other relevant quality attributes. The evaluation phase also provides feedback to the construction phase. A design artifact is complete and effective when the problem is solved. Table 1 gives methodologies for design evaluation. (Hevner at al 2004.)

This research process generated four publications and all of them have been evaluated by the acceptance processes of international conferences. Additionally, simulation was used in [P2] and field study in [P4]. The first publication [P1] was evaluated in a descriptive way.

Table 1 Methodologies for design evaluation (Hevner at al 2004)

1. Observational	Case Study: Study artifact in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation – Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Guideline 4 Research Contributions

The fourth guideline says that IS research must provide clear contributions in the research area. The IS design research can produce design artifacts, foundations or methodologies. The most important thing is that research process adds new information to the knowledge base. (Hevner at al 2004.)

This research process produced both descriptive and functional artifacts. Descriptive artifacts provide basic information about satellite based tracking systems. Functional artifacts present tools and methodologies for finding technical vulnerabilities in satellite based tracking systems. All results are publicly available in the databases of conferences.

Guideline 5 Research Rigor

The fifth guideline states that the design science research has to use rigorous methods in both the construction and evaluation of the designed artifact. Furthermore, overemphasis on rigor can lessen the relevance of IS design research because both the environment and the artifact itself can be informal. The rigor is achieved by the effective use of the knowledge base. However, the basic idea is to evaluate how well an artifact works, not prove why it works. (Hevner at al 2004.)

The main purpose of the knowledge base is that it is used as a toolbox and a researcher can use tools and information that solve the problem most efficient way. Many tools were used

during this research process. Especially the third publication [P3] combined many methodologies such as qualitative risk analysis, grounded theory and simulation. The first [P1] and second publication [P2] effectively combined existing information from the knowledge base. The last publication [P4] reused the information that was created in earlier publications.

Guideline 6 Design as a Search Process

The sixth guideline explains that abstraction and representation of means, ends and laws are components of design science research. Means are the set of actions and resources available to construct a solution and ends represent targets and constraints on the solution. Laws are uncontrollable forces the environment. When the means, ends and laws are realistic the design artifact becomes more relevant and valuable. (Hevner at al 2004.)

The target of this research was to find possible technical vulnerabilities for satellite based tracking systems and the problem space was wide as presented in chapter 2. The problem space did not contain strict limitations and we had to set limitations by ourselves, we decided to focus on telecommunications. The greatest limit on the research process was the time that was available for the research work.

Guideline 7 Communication of Research

The last guideline states that design-science research must be presented both to technology-oriented as well as management-oriented audiences. A technology-oriented audience need details to use the artifact within their implementation. A management-oriented audience needs information to evaluate if the artifact is usable in their organization. (Hevner at al 2004.)

The results of all the publications, except the journal [P2], were presented in conferences for scientific and technical oriented audiences. Publication [P1] was presented for the Saterisk management group and publication [P2] for the audience of other university. Continuous communication with research colleagues, audiences and lecturers provided self steering and added rigor in the research process.

The research process is summarized with the time schedule in figure 7.

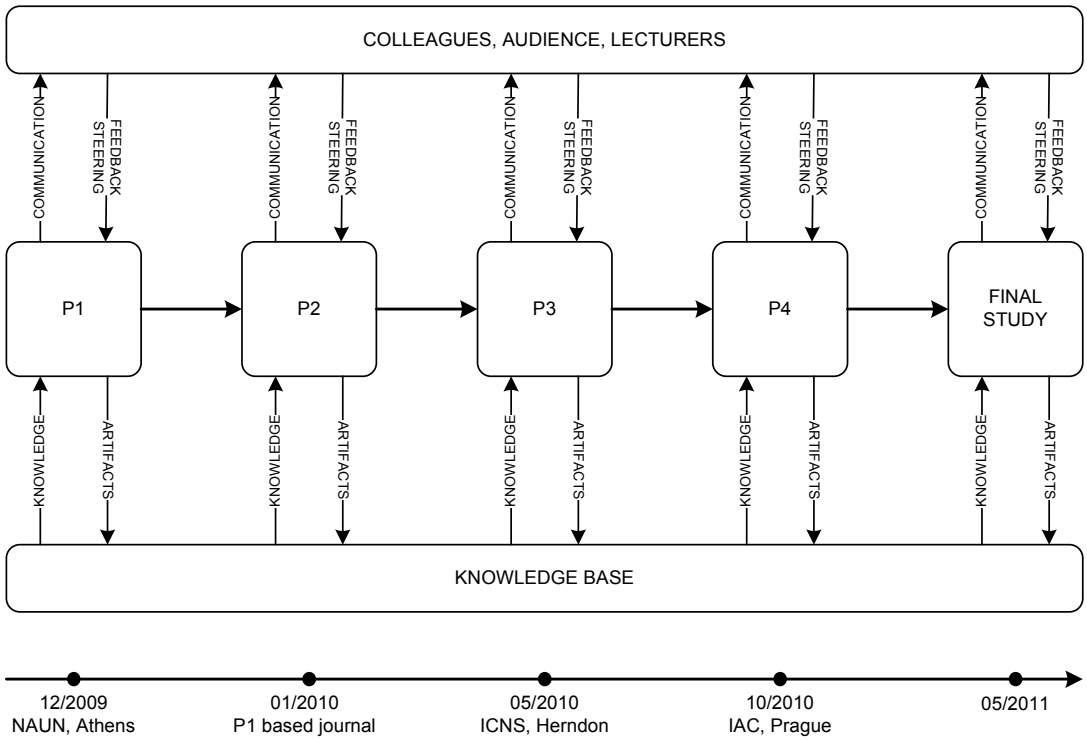


Figure 7 Research process with time schedule

4 Summary of Publications

4.1 Information security in satellite tracking systems

Commercial satellite based tracking solutions highlight the benefits for business but very rarely mention how their systems are protected against information security threats. The first publication [P1] and the second publication [P2] presents possible information security threats in satellite based tracking system and gives some guidelines how to make system less vulnerable.

Many commercial satellite based tracking systems are built on the top of commercial telecommunications networks. Telecommunications networks, like GSM and UMTS, have very limited features for end to end packet data protection. The data transfer path is secured in the air interface but only partially in the core network. In the internet the data path is fully unprotected. Additionally, a user does not know how a network operator has protected the network against security threats. (Kämppi at al 2009.) The data path is presented in figure 8.

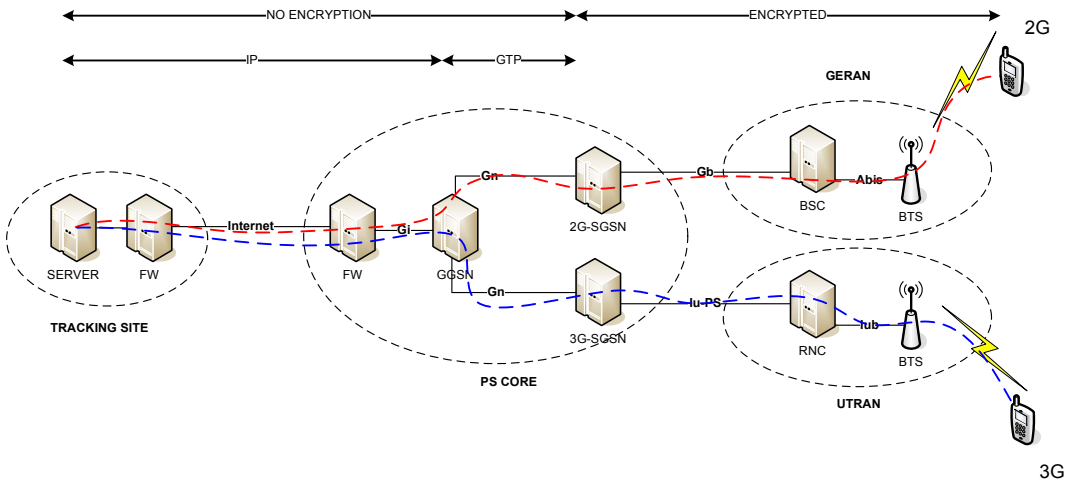


Figure 8 Routing of user data in mobile networks (Kämppi at al 2009)

The position data is processed and stored in a data center. The data center can be compared to a small corporate data center from the security point of view. If the data center is connected to the internet, it is vulnerable to many threats; denial of service (DOS) attacks, viruses, worms, pharming, cross scripting, and social engineering. (Kämppi at al 2009.)

In some commercial satellite tracking solutions, the data center is hosted by the service provider, so a user can not be sure how the positioning data is hosted. There are many open questions like: where is the data center located what kind of protection mechanisms are used, what is the professional level of personnel, and whether there is any co-operation with government? Therefore, the user has to be aware of what service is chosen. (Kämppi at al 2009.)

Commercial satellite tracking service providers have made matters easy by reusing smart phones as tracking devices. The user needs only to download a tracking application to the smart phone to use the smart phone as a tracking device. (Aspicore.) Smart phones can be compared to computers and they can have security vulnerabilities depending on the operating system used.

New operating systems for smart phones, like iOS by Apple and Android by Google, are fascinating but they are vulnerable too. Many security threats for these operating systems have been reported. (Apple 2010; Broersma 2010.) As the number of smart phones grows they become more interesting targets for the hackers too. Dedicated devices for satellite tracking are available, but their security vulnerabilities have not been investigated here.

End-users can access their positioning data via the internet, and their computers are vulnerable to all typical threats of the internet. How well their equipment is protected and main-

tained is fully dependent on the user. This can be a security risk for satellite tracking systems, if a attacker gains access to a hosting server by using stolen user accounts. (Kämppi at al 2009.)

The system can be protected by using existing technology and using known best practices. The data transfer path can be protected with secure tunneling or by encrypting data messages with a security algorithm. The data processing center needs professional personnel and good security equipment. Personal computers and smart phones can be protected with security suites that are offered by many software houses. (Kämppi at al 2009.)

As discussed in this paper, a satellite tracking system is quite a complicated system from the information security point of view. It contains parts of wireless and wired communication, and it is obvious that it contains information security risks if the system is not built properly. Securing the satellite tracking system the data path is especially important if the system is used to deliver sensitive positioning data.

4.2 Technical risk analysis for satellite tracking systems

In this publication [P3], we focused on creating a flexible model to determine the most severe technical risks in satellite-based tracking systems. This publication [P3] also extended the risk analysis to cover whole satellite based tracking system.

The purpose of risk analysis is not to eliminate all risks because this is rarely possible. Risk analysis is used to find out the most severe risks, and reduce these risks to an acceptable level (Peltier 2001, 23). Peltier divides risk analysis methodologies into two main streams; quantitative risk analysis and qualitative risk analysis (Peltier 2001, 19-20).

The target of quantitative risk analysis is to define a monetary or other numerical value for potential losses and determine the probabilities that such losses will occur for a given set of operations. It is often based on historical data, and the probability of a threat occurring is calculated by complex procedures. (Peltier 2001, 19-20.) Nevertheless, Sainsbury and Baskerville state that quantitative risk analysis is appropriate for frequently-occurring phenomenon, but it is particularly challenging when used to detect threats that are known but have never occurred (Sainsbury & Baskerville 2007).

The target of qualitative risk analysis is to define subjective definitions for potential losses and their associated likelihood of occurring. The severity and likelihood of potential losses can be described with terms like low, medium and high. Qualitative risk analysis can describe very rare threats or threats that have not been measured with quantitative risk analysis.

Peltier states that the qualitative risk analysis can provide useful results when the risk management team is competent and can assess the risks accurately. (Peltier 2001, 20).

Qualitative risk analysis was the best option for our research because we did not have historical data and our target was to find the most severe vulnerabilities without any limitations. We used the following steps of the Peltier´s practical methodology for qualitative risk analysis (Peltier 2001, 23-34).

1. Develop a scope statement
2. Form a competent team
3. Identify assets
4. Identify threats
5. Prioritize threats
6. Define impact priority
7. Calculate the total threat impact

Nonetheless, Peltier does not give any guidelines for categorizing threats and we combined the risk analysis process with Grounded Theory. Grounded Theory offers a methodology to categorize data and to investigate relations between categories (Charmaz 2006, 43-71). The method also encourages moving from the particular to the more general thinking (Bryant & Charmaz 2007, 14-17). The risk analysis process with Grounded Theory is presented in figure 9.

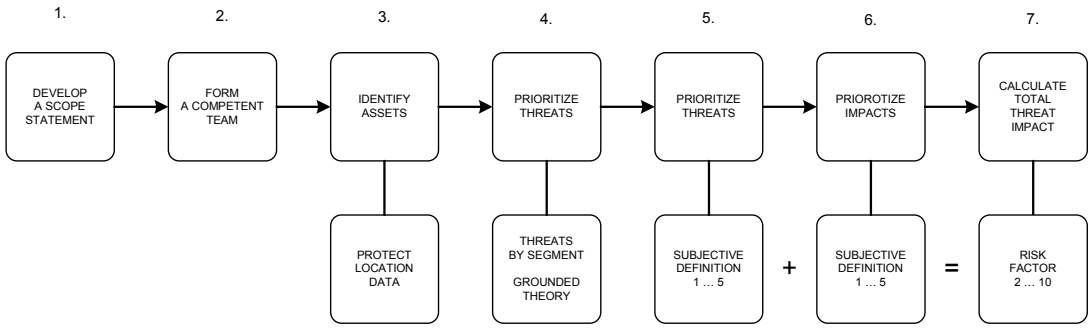


Figure 9 Qualitative risk analysis process

In order to avoid the problem of limited existing data or the limited knowledge of the risk analysis team, it is necessary to investigate the requirements of the applications and businesses too (Peltier 2001, 3). An application can have technical requirements that have not been levied on prior uses of the system. If the system can not offer a service with certain requirements, then it is a threat to the application. The requirements of the business can create technical requirements, and the technical limitations of the system causes threats to

those requirements being met. Using this approach, we were able to generate a model for identifying threats, shown in figure 10.

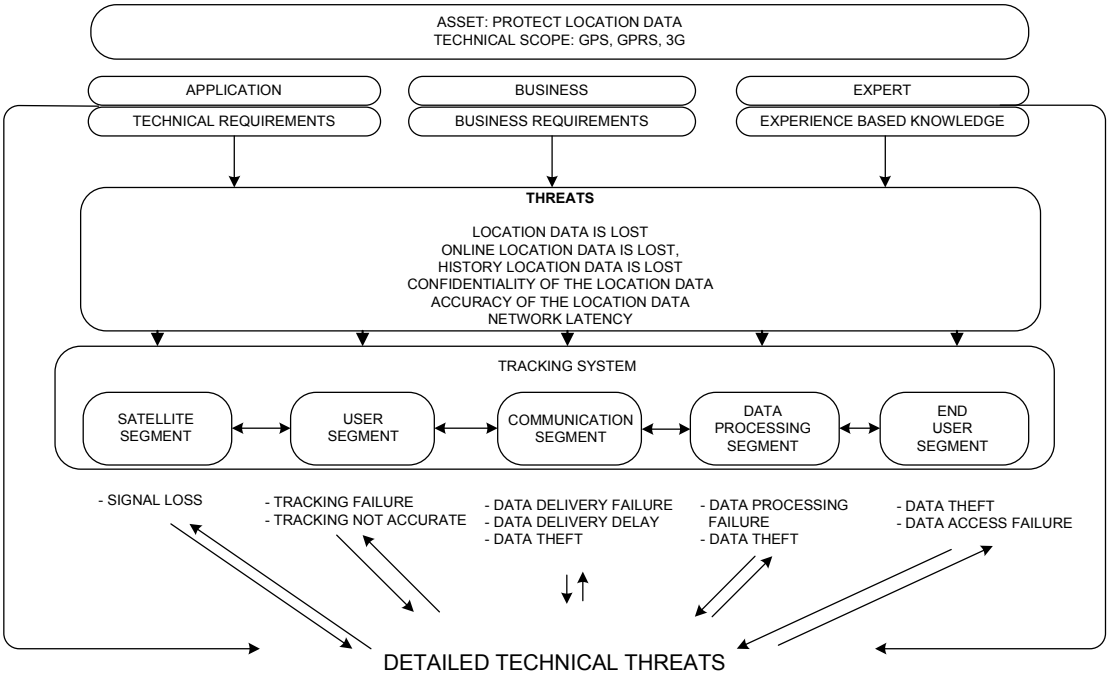


Figure 10 Model for identifying risks in satellite based tracking systems (Kämppi & Guinness 2010)

By using the model above we were able to define the list of the technical risks for each system segment. Threats are summarized by segment in table 2.

Table 2 Technical vulnerabilities in satellite based tracking systems

SYSTEM SEGMENT	THREATS
SATELLITE SEGMENT	UNINTENDED INTERFERENCE, INTENTIONAL INTERFERENCE, ATMOSPHERIC CONDITIONS, MULTIPATH PROPAGATION, SELECTIVE AVAILABILITY, TOTAL SIGNAL LOSS
TRACKING SEGMENT	HW FAULT, SW FAULT, POWER FEED BREAKDOWN, CLOCK DRIFT, SIGNAL ATTENUATION, INFORMATION SECURITY
COMMUNICATION SEGMENT	CAPACITY, RADIO COVERAGE, ROAMING, LATENCY, INFORMATION SECURITY
DATA PROCESSING SEGMENT	HW FAULT, SW FAULT, POWER FEED BREAKDOWN, CAPACITY, INFORMATION SECURITY, DATABASE CORRUPTION
END USER SEGMENT	INFORMATION SECURITY

4.2.1 Use cases

When the technical threats were defined we implemented an Excel-based tool for risk analysis. We also created three fictional use cases for the risk analysis tool simulation. The use cases were personal fitness and sporting activity, road toll Netherlands and the tracking of the cash in transit. Each use case had its own technical setup and different requirements for the tracking system. (Kämppi & Guinness 2010.) Subsequent sections present the risk profiles for the each use case.

Use case 1

Satellite tracking can be used to track personal fitness activities like jogging. Tracking client software can be installed into a smart phone and use a freeware tracking service that can be used via internet. (Kämppi & Guinness 2010.) Figure 11 presents the risk profile for personal fitness activity.

CATEGORY	THREAT	RISK FACTOR
DATA PROCESSING SEGMENT	HW-FAULTS	6
DATA PROCESSING SEGMENT	SW-FAULTS	6
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	6
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	6
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	6
USER SEGMENT	GPS - TOTAL SIGNAL LOSS	5
USER SEGMENT	DEVICE - HW-FAULTS	5
USER SEGMENT	DEVICE - SW-FAULTS	5
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	5
COMMUNICATION SEGMENT	INTERNET - CAPACITY	5
END USER SEGMENT	HOME USER - INFORMATION SECURITY	5

Figure 11 Risk profile for personal fitness activity (Kämppi & Guinness 2010)

After analyzing this use case, we evaluated the overall risk profile as medium. The most critical threats are found in the data processing and tracking segments (Kämppi & Guinness 2010).

Use case 2

The Netherlands has decided to deploy a road toll system that is based on driven kilometers (Mitchie 2008). The system will cover the whole of the Netherlands, and people are charged whenever they are driving a car. The location data is very crucial for the business, and location data must not be lost in any circumstances. The tracking device is able to buffer data if a network connection is lost. It is possible that some people are using jammers to avoid road tolls. (Kämppi & Guinness 2010.) Figure 12 presents the risk profile for the road toll.

CATEGORY	THREAT	RISK FACTOR
USER SEGMENT	GPS - UNINTENDED INTERFERENCE	8
SATELLITE SEGMENT	GPS - INTENTIONAL INTERFERENCE	8
USER SEGMENT	DEVICE - HW-FAULTS	8
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	8
COMMUNICATION SEGMENT	INTERNET - CAPACITY	8
COMMUNICATION SEGMENT	INTERNET - ENCRYPTION	8
DATA PROCESSING SEGMENT	HW-FAULTS	8
DATA PROCESSING SEGMENT	SW-FAULTS	8
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	8
DATA PROCESSING SEGMENT	INFORMATION SECURITY	8
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	8
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	8
END USER SEGMENT	HOME USER - INFORMATION SECURITY	8
END USER SEGMENT	PROFESSIONAL USER - INFORMATION SECURITY	8
SATELLITE SEGMENT	GPS - TOTAL SIGNAL LOSS	7
USER SEGMENT	DEVICE - SW-FAULTS	7
COMMUNICATION SEGMENT	GPRS - CAPACITY	7
COMMUNICATION SEGMENT	GPRS - ENCRYPTION	7
COMMUNICATION SEGMENT	GPRS - RADIO COVERAGE	6
COMMUNICATION SEGMENT	GPRS - ROAMING	6

Figure 12 Risk profile for road toll (Kämppi & Guinness 2010)

The overall risk profile for this use case was evaluated to be from medium to high. The use of intentional interference could be fatal for the system, and this particular risk is rated high on the scale. Problems with the tracking device could cause a loss of location data. The road tax is based on the data collected, and any problems in data processing could lead to unreliable billing. (Kämppi & Guinness 2010.)

Use case 3

Cash in transit can be tracked with a satellite-based tracking system. In a fictional case, cash in transit is tracked in the Helsinki capital area. Robbery is possible, and many criminals might be using jammers. Location data is very sensitive, and real-time tracking is mandatory. (Kämppi & Guinness 2010.) Figure 13 presents the risk profile for cash in transit.

CATEGORY	THREAT	RISK FACTOR
SATELLITE SEGMENT	GPS - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	GPRS - ENCRYPTION	9
COMMUNICATION SEGMENT	GPRS - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	3G - ENCRYPTION	9
COMMUNICATION SEGMENT	3G - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	INTERNET - ENCRYPTION	9
DATA PROCESSING SEGMENT	INFORMATION SECURITY	9
END USER SEGMENT	HOME USER - INFORMATION SECURITY	9
END USER SEGMENT	PROFESSIONAL USER - INFORMATION SECURITY	9
SATELLITE SEGMENT	GPS - TOTAL SIGNAL LOSS	8
DATA PROCESSING SEGMENT	HW-FAULTS	8
DATA PROCESSING SEGMENT	SW-FAULTS	8
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	8
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	8
USER SEGMENT	DEVICE - HW-FAULTS	7
USER SEGMENT	DEVICE - SW-FAULTS	7
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	7
COMMUNICATION SEGMENT	GPRS - CAPACITY	7
COMMUNICATION SEGMENT	3G - PACKET DATA CAPACITY	7
COMMUNICATION SEGMENT	INTERNET - CAPACITY	7
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	7

Figure 13 Risk profile for cash in transit (Kämppi & Guinness 2010)

The overall risk profile of this use case was rated from medium to high. We can see that the tool can be used to highlight the high risk of intentional interference and security threats for sensitive location data. (Kämppi & Guinness 2010.)

4.2.2 Lessons to be learned

The simulation gave us quite interesting results. We noticed that our tool was able to create the unique risk profile for each use case. In other words, it is not possible to create a general risk profile to cover all cases and risk analysis has to be made case by case. The model used to develop the tool described in this paper is very flexible. It is easy to add new navigation or telecommunications techniques to cover future needs.

Grounded theory is not widely used in information system research but there are a few cases where grounded theory has been combined with other research methods (Bryant & Charmaz 2007, 339-355). This publication shows that Grounded Theory can be combined with other methodologies with great results. Grounded Theory helps the team to understand complex systems and helps the team to look at the risk profile from a new view.

4.3 Field testing for satellite based tracking systems

Publications [P1], [P2] and [P3] investigated satellite based tracking system vulnerabilities with theoretical and qualitative research methodology. The last publication [P4] presents practical and more quantitative methodologies in a real life context. The last publication [P4] also presented the latest version of the system level description that was presented in chapter 2.

The target of the last research was to find out how a satellite based tracking system performs in real life. Data transfer reliability and position fix accuracy was chosen as performance metrics. The previous phases of the research gave us a good theoretical basis and we had good knowledge of how the system works. We also knew what theoretical vulnerabilities could be faced during the test session.

We decided to use a smart phone as a tracking device. The smart phone was equipped with commercial tracking application that had a very extensive feature set for logging and calculation of the position fix. We also found a tracking service that was free of charge and available via the internet. The tracking service offered very good possibilities for location data backup and downloads too. We used a Finnish telecom operator as a service provider. We supposed that a smart phone is not an optimal tracking device and we used a real GPS receiver with

data logging capability as a reference device in parallel with the smart phone. The combination of equipment and services offered us quite a comprehensive set of technology for field testing. The setup is described in figure 14.

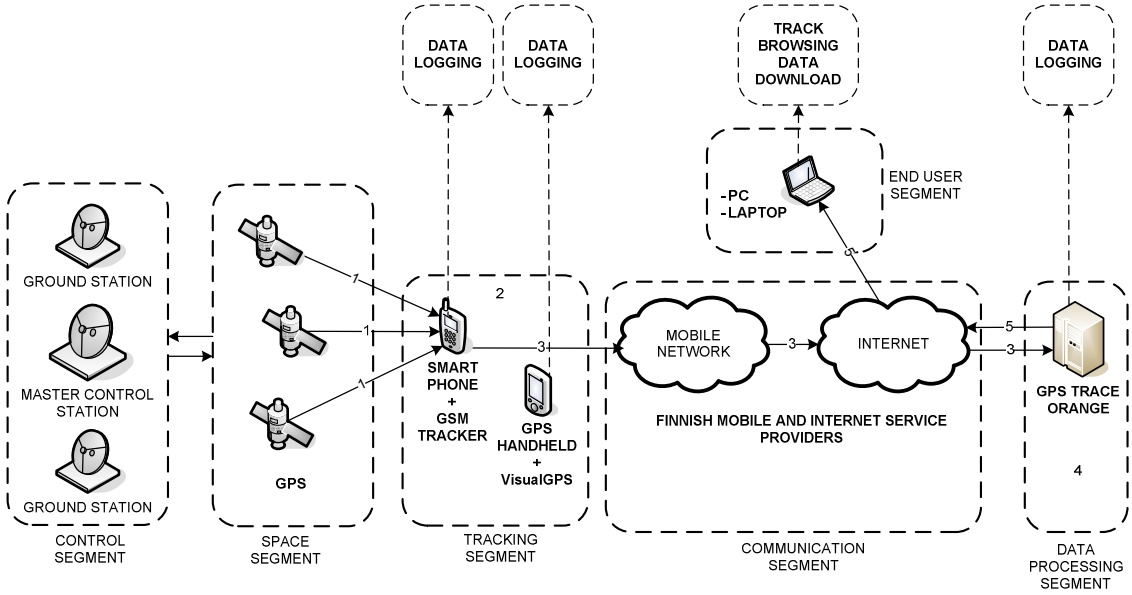


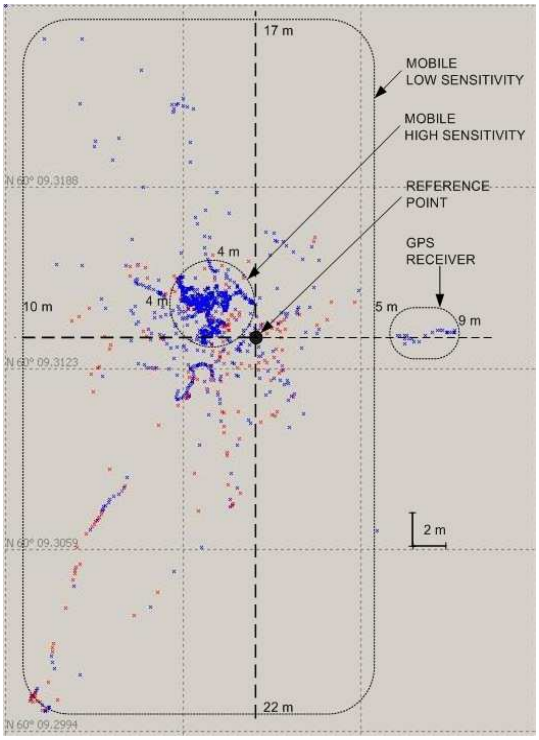
Figure 14 Field testing setup for a satellite based tracking system (Kämppi, Guinness & Urpila 2010)

We created five different types of test cases and our target was to emulate real use cases. The test cases were stationary tracking by car, rural and long haul tracking by car, urban tracking by car, open water tracking with a boat and bicycling. (Kämppi at al 2010.)

The location data was logged in the NMEA format. NMEA data format gives the coordinates of latitude and longitude, the number of detected satellites, the value of Horizontal Dilution of Precision (HDOP), the value of speed and much more. By comparing logged location data from both the tracking device and the tracking service we were able to calculate metrics for the data transfer reliability. The stationary accuracy was calculated by comparing logged location data to the coordinates of the known geographical position. We were also able to evaluate the precision of position fix by calculating the average for HDOP. (Kämppi at al 2010.)

The stationary test was executed with the smart phone and the GPS receiver. The setup provided us a possibility to compare results between two equipments. The results of testing revealed that the smart phone is not a perfect tracking device. The used smart phone has slide-out keyboard and GPS sensitivity is remarkable higher when the keyboard is exposed. The reason is that the GPS chip is located under the keyboard. (Kämppi at al 2010.)

The smart phone was able to detect 2 to 10 ten satellites when the GPS receiver detected 7 to 13 satellites in the same environment. The measured mean stationary longitude deviation of the smart phone in high sensitivity mode was 2.03 m and the mean stationary latitude deviation was 1.02 m. This observation does not directly reflect the accuracy expected because the measured sensitivity metrics (HDOP) were worse with the smart phone compared to the GPS receiver. (Kämppi at al 2010.) The reason could be software or hardware error in GPS receiver. Figure 15 shows the accuracy difference between the smart phone sensitivity modes and the GPS receiver.



Mobile low sensitivity = keyboard closed
Mobile high sensitivity = keyboard exposed

Figure 15 Accuracy difference between smart phone and GPS receiver (Kämppi at al 2010)

We found that data transfer reliability is 99.9 percent when the tracking device supports buffering in case that there are connectivity problems. The result is very good when we take into account the variety of the test cases. However, the test set was executed only in Finland and more testing is needed in an international environment. (Kämppi at al 2010.)

The overall functionality of the tracking system was very good but we found a few weak points too. Smart phone battery consumption is high when the GPS is activated and the battery will drain very fast if a continuous power feed is not available. This could be a limitation in some use cases. A smart phone is not suitable for the serious fitness usage either. The smart phone does not stand moisture or hard mechanical stress. (Kämppi at al 2010.)

We also found that an incoming circuit switched call can cause interruption for the active GPRS session and GPRS connection is suspended during a circuit switched call. This feature can cause interruption to the real time location tracking. If a tracking device supports buffering the tracking data is delivered to the tracking service when the GPRS connection is released from the suspension. (Kämppi at al 2010.)

One information security related vulnerability was found too. We noticed that it is possible to cause a service interruption to a single smart phone user by sending data to the user without user request. The network was not protected properly and our data load was routed to the mobile. The capacity was reserved from the radio interface and the internet connection of the mobile became unusable. A DOS attack could cause interruption to the real time tracking or the battery of the mobile phone will drain very fast. (Kämppi at al 2010.)

As a summary, we found that basic functionality is very reliable and the system level performance is quite good. In particular the modern telecommunication network can offer a reliable data transfer path for a satellite based tracking application. However, a smart phone can offer a satisfactory consumer level user experience with satellite based tracking service but in professional use it is more reasonable to consider other options. Dedicated tracking devices can offer more mechanical durability and they are not vulnerable to security risks as smart phones.

4.4 Contribution of the author

The first publication [P1] was written fully by the author but it was presented by Dr. Jyri Rajamäki at the conference. The idea for the publication was also originated by Dr. Rajamäki. The publication [P1] was reviewed by Dr. Rajamäki and Robert Guinness.

The second publication [P2] was written for a journal and was based on the first publication [P1]. The author conducted some additional research and Dr. Jyri Rajamäki edited the final version.

The third publication [P3] was written and presented by the author. Dr. Jyri Rajamäki, Robert Guinness and Tatu Urpila reviewed the publication. Guinness also made some editing work.

The last publication [P4] was produced through team work. The research and writing were done by the author and Robert Guinness. Tatu Urpila reviewed the paper and updated the references. The publication was presented by the author at the conference.

5 Conclusions and Discussions

5.1 Main results

The target of this research was to find the most critical technical risks of a satellite based tracking system. The research work was conducted as incremental research process and each publication presented new results for the final report. The form of results varies from theoretical descriptions to practical solutions.

The basis of system level analysis is to know how the system works and what technologies are involved. At the beginning of the research process we constructed the first version of a system description. We found that the system is complex and it combines many telecommunication, IT and navigation technologies. The system description is an essential part of each publication and it was improved during the research process. The last version of the system description presents seven system segments that have a specific role in the tracking chain.

The first [P1] and the second publication [P2] investigated information security related vulnerabilities in satellite based tracking systems. Commercial satellite based tracking services are usually built using commercial telecommunication networks, internet and IT services. The level of information security is not usually known and a user has to be aware if a tracking service is used for tracking sensitive or confidential targets. Location data can be captured by the third party if the data transfer path is insecure or the location data is stored in insecure place. The system is a potential target for denial of service (DOS)-attacks, viruses, worms, pharming, cross scripting, and social engineering too. A modern smart phone has integrated GPS functionality and the user should be aware if the smart phone is used as tracking device. New smart phone operating systems, like iOS by Apple and Android by Google, have security vulnerabilities and they will be interesting targets for criminals as the number of terminals grows.

The third publication [P3] presented a risk analysis procedure that was based on qualitative risk analysis and Grounded Theory. In qualitative risk analysis risk factors are based on the subjective definitions of risk analysis team. We found that the results are more reliable if the requirements of applications and business are taken into account too. Applications and business can have requirements that have not existed before and the risk analysis team is not familiar with them. We also created a risk analysis tool to simulate the analysis of three fictional risk analysis cases; personal fitness, road toll and cash on transit. The risk analysis tool was able to evaluate the risk factor for each technical threat on a scale from 2 (low) to 10 (high). The simulation rated the risk factor of the top five threats for personal fitness as 6, for road toll as 8 and for cash on transit as 9. Results show that each application and service

has requirements of their own and we can not create a general risk profile for all satellite based tracking applications. As a summary, reliable risk analysis requires cooperation with the risk analysis team, application developers and business people.

The last publication [P4] presented a real testing environment for satellite based tracking system. The environment was built using a smart phone, GPS receiver, commercial telecommunication networks and commercial tracking service. The target was to collect performance metrics and user experiences by executing test cases. The test cases were stationary tracking by car, rural and long haul tracking by car, urban tracking by car, open water tracking with a boat and bicycling. We found that that basic functionality is very reliable and the system level performance is good. Calculated data transfer reliability was 99.9% when the tracking device supported buffering. The measured mean stationary longitude deviation of the smart phone was 2.03 m and mean stationary latitude deviation was 1.02 m.

We also noticed that the mechanical design of a smart phone can have affect to GPS performance. The used smart phone has a slide-out keyboard and GPS sensitivity is significantly higher when the keyboard is exposed. The reason is that the GPS chip is located under the keyboard. The smart phone was able to detect 2 to 10 ten satellites when the GPS receiver detected 7 to 13 satellites in the same environment. Our testing revealed two vulnerabilities for real time tracking too. Real time data transfer can be interrupted by incoming circuit switched call or by sending dummy data the mobile from the internet host. These vulnerabilities were not found by theoretical risk analysis.

5.2 Discussion of the results

The first publication [P1] was written at the end of 2009 and then we raised the issue of smart phone information security. At that time Symbian was the dominant smart phone operating system and the other ones such as, iOS and Android, were challengers. Nobody knew the vulnerabilities of the new operating systems. After one year iOS and Android have extended their market share and the market share of Symbian has declined. Lately 65 security vulnerabilities have been reported for iOS and 88 security vulnerabilities for Android 2.2 (Apple 2010; Kingsley-Hughes 2010). The rising trend of discovered security vulnerabilities confirms our observation that was made in [P1]; users have to be careful with their smart phones if they are used with business critical applications.

The third publication [P3] analyzed the technical risks of satellite based tracking systems. We observed that the requirements of applications and business have a strong relation to the risk profile. The observation is in line with the guidelines of IS design research. IS design research states that people, organizations and technology create business needs (Hevner at al 2004). In other words, when the system is designed according to needs then most of the technical risks

could be avoided too. [P3] also presented intentional and unintentional interference as a technical threat to the satellite segment. The threat is real and it has lately raised a few interesting issues about possible interference scenarios. Dr. Parkinson presented at IAC 2010 conference that all existing navigation systems (GPS, GLONASS) and the new ones (Galileo, COMPASS) are using same L1 frequency. The use of the same frequency could cause interference problems if the systems are not designed properly. (Parkinson 2010.) Another recently reported case covered the telecommunication system and GNSS interworking. Physorg.com reported on Feb 2010 that the 4G (LTE) network by Lightsquared will cause interference to the GPS signal in US because they are using almost same frequency. The results of the simulation showed that the interference will start at 22.1 km for the aviation receiver and total signal loss occurred at 9.0 km from the transmitter. (Edwards 2011).

The last publication [P4] considered a field testing scenario for satellite based tracking and gave us real hands on experience of system performance. We found that the system performs very reliably in different use cases. In particular data transfer reliability in commercial telecommunication network was almost 100%. The testing period also revealed vulnerabilities that were not found through theoretical risk analysis. That observation shows that the testing period is an essential part of the system evaluation process and cannot be bypassed in any circumstances. Especially previously presented interference scenarios will require a proper field testing period.

5.3 Discussion of the research process

The objective of this research was to find the most critical technical risks for satellite based tracking systems. The emphasis was on system analyzing and evaluation, not on system development. Furthermore, testing and analyzing tools were developed during the research process as well.

A multimethodological approach for IS research recognizes four different phases for research; theory building, observation, experimentation and systems development (Nunamaker at al 1991). All these phases are used in research process. Each publication started with a theory building phase. In the theory building phase we developed new ideas and set our objectives. In the observation phase we integrated new knowledge with the research domain and that was made mainly in publications [P1], [P2] and [P3]. Publications [P1] and [P2] integrated information security related issues with satellite based tracking systems. The third publication [P3] integrated the deeper knowledge of telecommunications and satellite based navigation with the research domain. For example the system description was developed in the observation phase. The last publication [P4] presented results that were found with real satellite based tracking system in the experimentation phase. The last publication [P4] also reused

effectively the results of previous publications in experimentation phase. As mentioned earlier, we did not make system development for satellite based tracking system but we developed analysis tools in the system development phase. As a summary, the emphasis of the research process moved from theory towards practical experiments.

The research process was evaluated according to the guidelines for IS research. Hevner at al state that the research has to solve a meaningful problem, provide clear contributions in the research area, use rigorous research methods and the results have to be communicated to the audience properly. (Hevner at al 2004). The problem space for this research was defined by the Saterisk project. In other words, there was a real need to do this study and previous studies covered the problem space from a different angle. The research provided both theoretical and practical contributions; a system description for satellite based tracking systems, the list of found technical vulnerabilities, the prototype of a risk analysis tool, and measured performance metrics for a real satellite based tracking system. According to Hevner the researcher has to use rigorous research methods (Hevner at al 2004). The third publication presented how grounded theory was integrated with qualitative risk analysis and the fourth publication [P4] presented performance metrics that were achieved by field testing. Additionally, the contributions of publications [P1], [P3] and [P4] were presented for scientific audiences at international seminars.

5.4 Limitations

The scope of the research was very wide and many issues were studied. The satellite based tracking system combines many technologies and we concentrated on telecommunications and IT technologies. This was a natural choice because the author has been working with telecommunication systems for over ten years.

Our research covered satellite based navigation systems on a general level. We were able to recognize technical threats that are common to all satellite based navigation systems but we did not investigate if some of navigation system is more vulnerable compared to the other ones. Our system description improved during the research process and the system description did not the cover control segment and external applications in [P3]. The latest improvements were added to the system description in the last publication [P4]. Nevertheless, this does not lessen the results of [P3] because all previous system segments still exist in the final system description in [P4]. Anyway, our model for technical risk analysis is very flexible and recognized limitations could be added into the model easily.

The test cases of field testing were executed only in Finland and mainly in a rural environment. The quality of the telecommunication networks may vary in different countries and the results of data transfer quality metrics are not directly comparable to the international envi-

ronment. The focus of GPS performance testing was on stationary testing in an open environment. The next phase for GPS performance could be more specific testing in an urban environment.

5.5 Topics for future research

The research area was very interesting and new ideas and research questions came out all the time. That phenomenon shows that there is still some work to do in research area.

The risk analysis procedure was used with simulated cases during this research. The same procedure could be used with real applications and use cases to gain knowledge about real use cases.

This research covered information security related issues and data transfer quality metrics for legacy telecommunications networks (GPRS, 3G). The Finnish Police uses TETRA telecommunication systems in their daily routines but the technical vulnerabilities or performance as not yet been investigated by Laurea UAS. The field testing procedure could be useful for measuring quality metrics for TETRA networks too.

As discussed previously, it is possible that new satellite navigation systems (Galileo, COMPASS) could cause interference in existing systems (GPS, Glonass) if interworking is not designed properly. This indicates that the features of new satellite navigation have to be studied properly and more research is needed.

References

Books and publications

Bryant, A. & Charmaz, K. 2007. The SAGE Handbook of Grounded Theory. London: SAGE.

Charmaz, K. 2006. Constructing Grounded Theory. London: SAGE.

Happonen, M. 2010. Recognizing risks of satellite based tracking. Espoo: Laurea UAS.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. MIS Quarterly. Volume. 28 Issue.1.

Kokkonen, P. 2010. Paikannus merellä lain ja tekniikan näkökulmasta. Espoo: Laurea UAS

Kämppi, P., Rajamäki, J. & Guinness, R. 2009. Information security in satellite tracking systems. Athens: 3rd International Conference on Communication and Information Technology.

Kämppi, P. & Guinness, R. 2010. Technical Risk Analysis for Satellite Based Tracking Systems. Herndon: Integrated Communications Navigation and Surveillance Conference (ICNS).

Kämppi, P., Guinness, R. & Urpila, T. 2010. Field Testing for Satellite Based Tracking Systems. Prague: 61st International Astronautical Congress.

Nunamaker, J., Minder, C. & Purdin, T. 1991. Systems Development in Information Systems Research.

Peltier, T. 2001. Information Security Risk Analysis. CRC Press LLC.

Sainsbury, R. & Baskerville, R. 2007. Possible Analysis Engine: A prototype Tool for Managing IT Security Safeguards Acquisition. California: Forthcoming in The International Conference on Information Warfare and Security

Viitanen, J. 2009. SATERISK-projektin suunnittelu ja vaatimusmäärittely. Espoo: Laurea UAS.

Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. 2009. International and Transorganizanional Information Flow of Tracking Data. Tenerife: 8th WSEAS International Conference On Information Security and Privacy.

Electronic references

3GPP. GPRS & EDGE. Referred on 23.02.2011. http://www.3gpp.org/article/gprs-edge

3GPP. HSPA. Referred on 26.02.2011. http://www.3gpp.org/HSPA

3GPP. LTE. Referred on 26.02.2011. http://www.3gpp.org/LTE

3GPP. Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0. 2009. Referred on 26.02.2011. http://www.3gpp.org/ftp/Specs/html-info/23040.htm

3GPP. UMTS. Referred on 26.02.2011. http://www.3gpp.org/article/umts

About.com. 2000. President Turns Off GPS Selective Availability. Referred on 26.02.2011. http://geography.about.com/library/weekly/aa050400a.htm

Apple. 2010. About the security content of iOS 4. Referred on 26.02.2011. http://support.apple.com/kb/HT4225

Aspicore. Aspicore GSM Tracker. Referred on 26.02.2011. http://www.aspicore.com/en/tuotteet_tracker.asp

Broersma, M. 2010. Serious Security Bugs Found in Android Kernel. eWEEKeurope. Referred on 26.02.2011. http://www.eweekeurope.co.uk/news/serious-security-bugs-found-in-android-kernel-11040

Edwards, L. 2011. New 4G network could cause widespread GPS dead zones. Physorg.com. Referred on 07.04.2011. http://www.physorg.com/news/2011-02-4g-network-widespread-gps-dead.html

European Space Agency. Who´s involved in Galileo. Referred on 26.02.2011 http://www.esa.int/esaNA/GGG28850NDC_galileo_0.html

European Space Agency. Why Europe needs Galileo. Referred on 26.02.2011 http://www.esa.int/esaNA/GGG0H750NDC_galileo_0.html

European Space Agency. What is Galileo. 2010. Referred on 26.02.2011. http://www.esa.int/esaNA/GGGMX650ND_C_galileo_0.html

GpsGate.com. Developer´s Guide GpsGate api. Referred on 26.02.2011. http://gpsgate.com/go/gpsgate/dev_guide.asp

GpsGate.com. Gpsgate Client. Referred on 26.02.2011. http://gpsgate.com/products/gpsgate_client

GPSworld. High Integrity Navigation. Referred on 26.02.2011. http://www.gps-world.biz/products/highinteg.php

GSM World. GSM. Referred on 24.02.2011. http://www.gsmworld.com/technology/gsm/index.htm

Inside GNSS. About GPS. Referred on 23.02.2011. http://www.insidegnss.com/aboutgps

Inside GNSS. About Glonass. Referred on 23.02.2011. http://www.insidegnss.com/aboutglonass

Inside GNSS. About Galileo. Referred on 26.02.2011. http://www.insidegnss.com/aboutgalileo

JAMMER WORLD. Referred on 05.03.2011. http://www.thejammerworld.com/

Kingsley-Hughes. 2010. 88 'High Risk' vulnerabilities discovered in Android 2.2 'Froyo'. Referred on 08.03.2011. http://www.zdnet.com/blog/hardware/88-high-risk-vulnerabilities-discovered-in-android-22-froyo/10217

Kowoma.de. 2009. Control Segment. Referred on 26.02.2011. http://www.kowoma.de/en/gps/control_segment.htm

Kowoma.de. 2009. History of NAVSTAR GPS. Referred on 26.02.2011. http://www.kowoma.de/en/gps/history.htm

Kowoma.de. 2009. GPS Satellites. Referred on 26.02.2011. http://www.kowoma.de/en/gps/satellites.htm

Kowoma.de. 2009. GPS Satellite orbits. Referred on 26.02.2011. http://www.kowoma.de/en/gps/orbits.htm

Kowoma.de. 2009. Position Determination with GPS. Referred on 26.02.2011.

http://www.kowoma.de/en/gps/positioning.htm

Michie, B. 2008. Dutch GPS Toll Update. Eroad. Referred on 04.04.2011. http://www.eroad.com/dutch-gps-toll-update/

Motorola. Tetra terminal MTP850. Referred on 26.02.2011. http://www.motorola.com/Business/XU-EN/Product+Lines/Dimetra+TETRA/TETRA+Terminals/MTP850_XU-EN_PK-EN_XF-EN

National Aeronautics and Space Administration, Spacewarn Bulletin. 2010. Spacewarn Bulletin. Referred on 04.04.2011. http://nssdc.gsfc.nasa.gov/spacewarn/spx681.html

Parkinson, P. 2010. Conference plenary, Never Lost Again. Prague: 61st International Astronautical Congress. Referred on 03.03.2011. http://www.iafastro.com/index.html?title=IAC2010_Plenary_3

PCMAG.COM. Definition of API. Referred on 26.02.2011. http://www.pcmag.com/encyclopedia_term/0,2542,t=application+programming+interface&i=37856,00.asp

Phone.com. 2009. TeliaSonera launched LTE (4G) networks in Scandinavia. Referred on 26.02.2011. http://www.phones.com/news/teliasonera-launched-lte-4g-networks-scandinavia/

SATCOM TECHNOLOGY. Fleet Management. Referred on 05.03.2011. http://www.satcomtechnology.com/tracking-solutions/fleet-management

SATCOM TECHNOLOGY. Anti Hijack. Referred on 05.03.2011. http://www.satcomtechnology.com/wp-content/uploads/2010/02/Anti%20Hijack.pdf

SkyToll. Technology. Referred on 26.02.2011. https://www.emyto.sk/web/guest/technology

Stanford News Service. 1995. A brief history of satellite navigation. Referred on 26.02.2011. http://news.stanford.edu/pr/95/950613Arc5183.html

The Slovak Spectator. 2009. Electronic road toll system to replace stickers. Referred on 05.03.2011. http://spectator.sme.sk/articles/view/34446/23/electronic_road_toll_system_to_replace_stickers.html

Velocitybox. GPS data loggers. Referred on 26.02.2011. http://www.velocitybox.co.uk/index.php/en/products/gps-data-loggers?gclid=CNOH8dC-pacCFcKlDgodpn0WCw

TETRA Mou Associaton. Markets & Applications. Referred on 26.02.2011. http://www.tetramou.com/tetramou.aspx?&id=2237

TETRA Mou Associaton. Key Services. Referred on 26.02.2011. http://www.tetramou.com/tetramou.aspx?&id=2229

TETRA Mou Associaton. Tetra Release 2. Referred on 26.02.2011. http://www.tetramou.com/tetramou.aspx?&id=1186

TRACK24. ROADRUNNER. Referred on 05.03.2011. http://www.track24.co.uk/products_hardware_vehicles_roadrunner/#specifications

Urban Traffic Control Centre of Helsinki. 2008. Renewal of HeLMI. Referred on 05.03.2011. http://www.hel2.fi/liikenteenohjaus/helmi/uudistus2008.asp

Urban Traffic Control Centre of Helsinki. 2007. New Public Transportation Sensor. Referred on 05.03.2011. http://www.hel2.fi/liikenteenohjaus/helmi/uusi_joukkoliikenneilmaisin.asp

U.S Air Force. 2010. Airmen upgrade GPS constellation. Referred on 23.02.2011. http://www.af.mil/news/story.asp?id=123207262

WiMax.com. What is WiMAX. Referred on 26.02.2011. http://www.wimax.com/general/what-is-wimax

WIMAX Forum. 2011. Monthly Industry Report, February 2011. Referred on 26.02.2011. http://www.wimaxforum.org/resources/monthly-industry-report

Russian Federal Space Agency, Information-Analytical Centre. 2011. GLONASS constellation status. Referred on 23.02.2011. http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:20:1322200481925923::NO

Appendices

Appendix 1: Publication [P1], Information security in satellite tracking systems
Appendix 2: Publication [P2], Information security for satellite tracking systems
Appendix 3: Publication [P3], Technical Risk Analysis for Satellite Based Tracking Systems
Appendix 4: Publication [P4], Field Testing for Satellite Based Tracking Systems

Publication P[1]

P. Kämppi, J. Rajamäki, R. Guinness, Information security in satellite tracking systems, 3rd International Conference on Communication and Information Technology, Athens, Greece, Dec 2009, ISBN: 978-960-474-146-5, pp. 153-157.

Information security in satellite tracking systems

Pasi Kämppi, Jyri Rajamäki, Robert Guinness

***Abstract*—**Satellite tracking is one of the most rapidly growing business areas in the world, and there are already many commercial applications available. Benefits for the customer are advertised, but there is no mention of information security. Modern satellite tracking systems contain communication on many levels, so they are vulnerable to many risks of information security. This paper covers the main satellite tracking system information security vulnerabilities and gives guidelines on how to make systems more secure.

***Keywords*—**Information security, Internet, Mobile network, Satellite tracking

I. Introduction

Satellite tracking is one of the most rapidly growing business areas in the world. Tracking devices have become quite cheap, and they are available to nearly everybody. Even smart phones can be used as tracking devices.

During the last decade, mobile network coverage has also grown, and internet has become as part of our everyday life. This evolution has enabled the innovation of new solutions, and one of them is the satellite tracking system.

Risks of satellite tracking have not been investigated widely, so a few students of Laurea University of Applied Sciences started to make preliminary research in 2008. Research on the technical risks of satellite tracking systems continued in 2009, and this paper describes one part of this larger research work.

This research revealed that information security in satellite tracking systems is not guaranteed, and this paper describes major vulnerabilities and gives some guidelines on how information security can be improved.

II. SATELLITE TRACKING SYSTEMS

Modern satellite tracking systems consist of many technical segments: the satellite segment, communication segment, data processing segment, and end-user segment. The basic principle is that the tracked device is positioned by satellites, and the positioning data is delivered for post-processing via mobile networks and the internet. This principle is shown in Fig. 1.

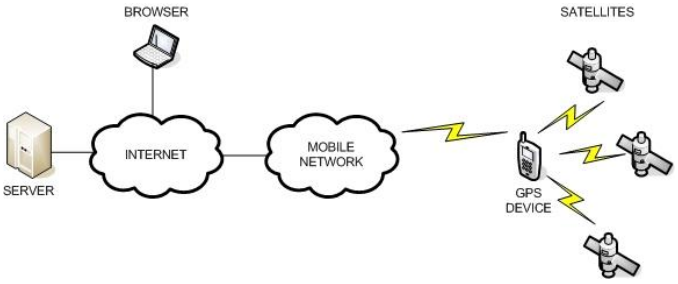


Fig 1 Principle of a satellite tracking system

A. Satellite segment

The satellite segment contains techniques to calculate the device's position from satellite signals.

1) GPS

The most commonly used satellite positioning system is the Global Positioning System (GPS) [1]. It has been developed by the U.S. military, but service is also available for civilian usage. The system consists of 24-32 active satellites, and it covers whole world. Since the U.S. government stopped intentionally degrading the signal in 2000, the position data provided by GPS is quite accurate.

2) GLONASS

GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) [1] is developed and used by Russia. The system is like GPS, and it should be able to offer as accurate as position service as GPS. In practice, the number of satellites operating in the GLONASS constellation has been quite low (8-12), so the service is as accurate as GPS. The satellite constellation is optimized so that usability is best behind Russian borders.

3) GALILEO

GALILEO [1] is under development by EGNOS (European Geostationary Navigation Overlay Service). EGNOS is project that is sponsored by ESA (European Space Agency) and the European Commission. The goal of this project is to develop navigation service for civilian usage, independent of the military. GALILEO is technically like GPS and GLONASS, and some devices will be able to utilize all three

Manuscript received December 14, 2009. This work was supported in part by Laurea University of Applied Sciences and by Tekes – the Finnish Funding Agency for Technology and Innovation.

P. Kämppi, J. Rajamäki and R. Guinness are with the Laurea University of Applied Sciences, Espoo, Vanha Maantie 9, 02650 Finland (corresponding author to provide phone: 358-50-5140823; (e-mail: pasi.kamppi@ laurea.fi).

systems. In this way, several techniques can be used simultaneously to guarantee better positioning accuracy and reliability.

B. Communication segment

The communication segment contains techniques to deliver positioning data for post-processing and use by end-users. The most commonly used techniques are offered by mobile networks, namely the General Packet Radio System (GPRS) [2] and Short Message Service (SMS) [3]. The internet is used to route positioning data from mobile networks for post-processing, and this makes the system globally available. End-users can access their data via the internet as well.

C. Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data. End-users can access their services via the internet, so systems have to be connected to internet safely and reliably.

D. End-user segment

The end-user segment offers customer interfaces for their positioning data. Typically interfaces are offered via internet connection and web browser.

III. MOBILE NETWORK USER PLANE SECURITY

A. History

Originally GSM (Global System for Mobile communications) [4] did not offer as advanced data services as they currently do. In the first phase, there was Circuit Switched Data (CSD), followed by High Speed Circuit Switched Data (HSCSD) [5] that offered four times faster access rate compared to CSD. Common for these services is that they use communication channels based on Time-Slot Leasing (TSL) sheme.

General Packet Radio Service (GPRS) was the first packet-switched mobile network service that offered internet-like end-user experience. In its first phase, GPRS was quite slow and network delay was large. GPRS was followed by Enhanced Data Rates for Global Evolution (EDGE) [6], and it offered faster user data rate and smaller Round Trip Time (RTT).

Universal Mobile Telecommunications System (UMTS) [7] offers end-user data rates that make as real mobile internet experience as possible. Modern systems are upgraded with High Speed Downlink Packet Access (HSDPA) [8], and this type of mobile internet connection is comparable to a fixed connection in terms of data rate.

Common to all these development phases is a focus on developing faster networks, but mobile networks do not natively provide secure end-to-end user plane data transfer features.

B. GPRS

Originally GPRS was built on top of the GSM network infrastructure with a few additional network elements, and it reuses the majority of the existing network architecture. Later networks were upgraded with UMTS, and a few new network elements were introduced. Logical architecture of GPRS network is described in 3GPP TS 23.060 V9.2.0, as shown in Fig 2.

On the Base Sub System (BSS) and UMTS Terrestrial Radio Access Network (UTRAN), user plane data can be encrypted between Mobile Station (MS) and Service GPRS Support Node (SGSN). BSS supports GPRS Encryption Algorithm (GEA) and UTRAN supports UMTS Encryption Algorithm (UEA). Equipment is now available that can break ciphering from the air interface, so it is possible to capture data before it enters BSS or UTRAN.

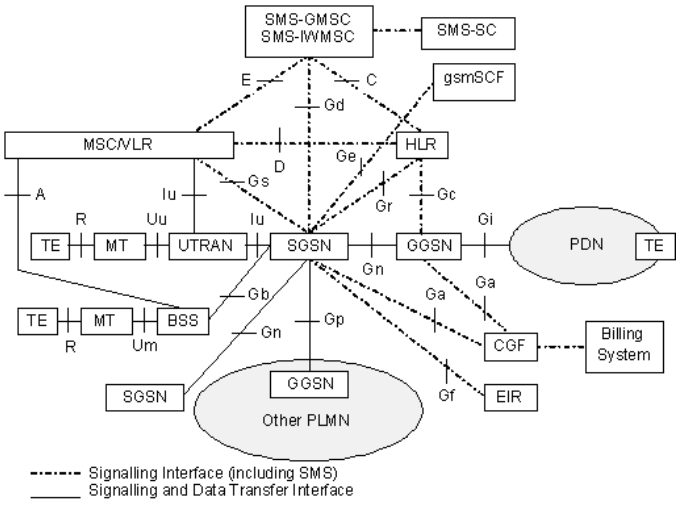


Fig 2 GPRS Logical Architecture

When data continues towards GPRS Gateway Support Node (GGSN), then data is encapsulated with GPRS Tunneling Protocol (GTP) [9] over IP. GTP does not support any encryption features. In practice, data is transferred as plain text, and it can be captured quite easily if the intruder has access to the backbone. GTP is used between operators as well, and it is quite vulnerable if traffic is routed via an insecure internet connection. From GGSN, data continues towards the internet, and then data is available to anybody. Data flow is presented in Fig 3.

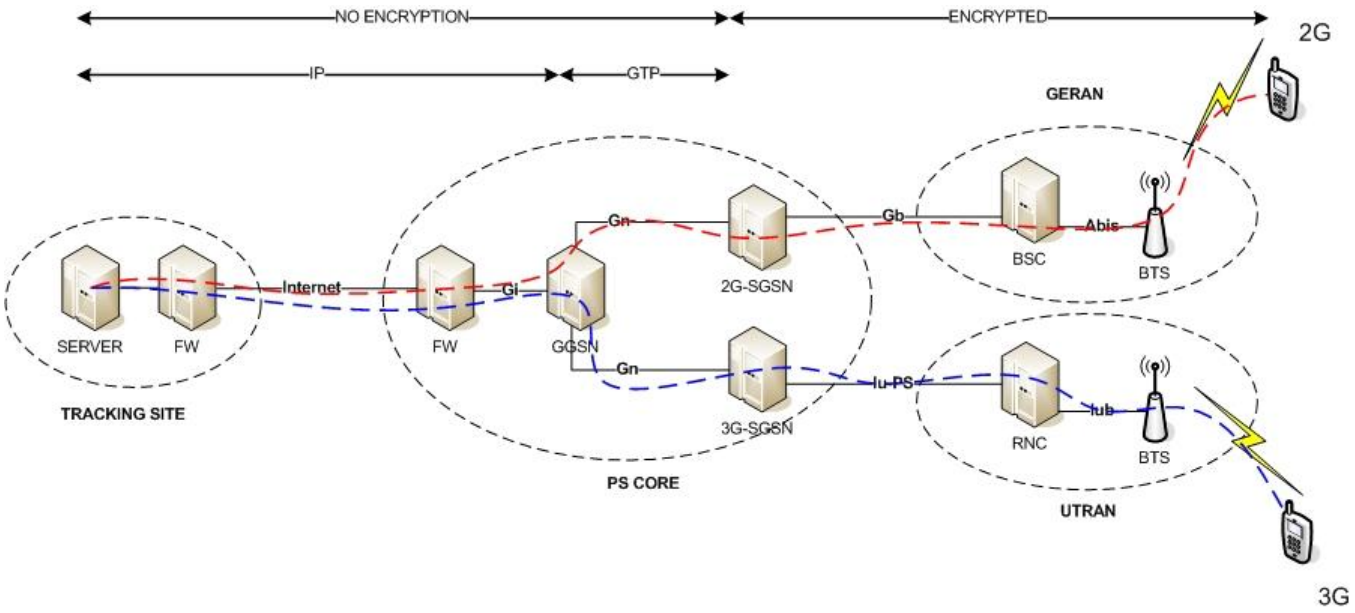


Fig 3 Data flow in GPRS

C. *Short Message Service*

Short message service (SMS) provides a method to send short messages via mobile networks [3]. Messages are delivered using signaling, and they are encrypted only in the air interface. After BSS and UTRAN they are transferred as plain text. From BSS and UTRAN the message continues towards the Mobile Switching Center (MSC) and Short Message Center (SMSC).

Globally networks of different operators are connected with Signaling System Seven (SS7) [10], so short messages are delivered between operators using SS7 as well. SS7 does not support any security functions, so it is possible to capture messages from the operator network if somebody is able to break in. Nowadays SS7 can be carried over IP, and this makes SS7 even more vulnerable if signaling between operators is routed via an insecure internet path. On the internet, signaling data is available for anybody.

In satellite tracking systems, positioning data is delivered for post-processing by a machine to machine (M2M) interface. Typically these interfaces (e.g. CIMD2) do not support any security functions, and data can be routed via an insecure internet path.

D. *Security solutions*

As discussed above, it is quite obvious that positioning data can not be carried safely via mobile networks. Globally there are many different operators with different information security practices, so the end-user can not rely on data being delivered safely. In the most blatant case, when data enters the internet, then it is available to anybody.

1) *Data protection with GPRS*

Data can be protected by establishing secure tunneling between the client and data processing center. By secure tunneling, we can make data transfer as secure as the chosen encryption method is. The most common technique is IP Secure Architecture (IPsec).

2) *Data protection with SMS*

Due to the fact that SMS is delivered in mobile network signaling, it can not be secured by tunneling like GPRS data. SMS is plain text, so it can encrypted before sending by using Secure Hash Algorithms (SHA), such as SHA-256, SHA-384, or SHA-512.

IV. DATA CENTER SECURITY

Position data is processed and stored in a place that can be compared to a small corporate data center from the security point of view. A data center is typically connected to the internet, so it is vulnerable for many threats like denial of service (DOS)-attacks, viruses, worms, pharming, cross scripting, and social engineering.

In some commercial satellite tracking solutions, the data center is hosted by the service provider, so the user can not be sure how positioning data is hosted. There are many open questions like: Where is the data center located, what kind of protection mechanisms are used, what is the professional level of the personnel, and is there any co-operation with government? Therefore, the user has to be aware of what service is chosen.

A. Security threats

1) Denial of service -attacks

The aim of denial of service attacks [11] is to make a website unavailable. A website can be overloaded by the attacker, and users will not be able to access their data.

2) Viruses

A computer virus is a small applet that needs a host program for spreading. Usually their purpose is to cause some harm to the infected system.

3) Worms

Worms are small applications that can spread independently in networks and execute code autonomously. Their goals are to cause disasters, open new security holes, and steal data.

4) Pharming

Pharming [12] is an attack in which a user is directed to a fake website instead of the real one. The user does not notice that they are at the fake website, so sensitive information like username and password can be stolen. Another term for this threat is "DNS cache poisoning".

5) Cross site scripting

Cross site scripting (XSS) [13] is a WWW-server vulnerability where the attacker can execute code in the HTTP address or via an interactive webpage. The purpose can be to steal data or usernames.

6) Social engineering

Social engineering is a method in which somebody is tricked into giving sensitive information to the attacker. This is a very common way to discover data about a company.

B. Security solutions

There are many security threats when services are available via the internet and only a few have been introduced here. The main way service providers can protect their users is to be aware of these threats and make the system as secure as possible.

1) Best practices

There are many guides that include instructions on how to create secure network, for example, RFC2196 Site Security Handbook [14] and Standard of Good Practice for Information Security [15].

2) Personnel

Information security is an area where knowledge has to be updated frequently. Personnel have to be aware about possible threats, which can be achieved by proper training.

3) Security equipment

Corporate networks can be secured with additional equipment like firewalls, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). A well-planned security solution is built by using all of them as needed.

4) Operating systems

It is important to keep operating system software updated. There are frequent new software releases, and maintenance personnel have to be aware of these updates. Operating systems can be "hardened," meaning that all unnecessary services all disabled.

V. CLIENT SECURITY

Commercial satellite tracking service providers have made matters easy by reusing smart phones as tracking devices. The user needs only to download a tracking application to turn his or her smart phone into a tracking device. Smart phones can be compared to computers in that they can have security vulnerabilities depending on the operating system used.

Dedicated devices for satellite tracking are available, but their security vulnerabilities have not been investigated here.

A. Symbian OS

Symbian [16] is probably the most widely-used smart phone operating system in the world. Because it is like a computer, it has many vulnerable interfaces.

Threats can occur via downloadable applications, GPRS, SMS, web browser, or email. In theory, it is possible that a mobile can be hijacked and managed remotely to direct positioning data to a place available to the attacker.

B. iPhone

The iPhone [17] is the newcomer in the mobile world, and there has already been a few severe security threats reported. It has been possible to capture iPhone data via SMS [18], and the first worms [19] have also been spread among iPhones.

C. Other operating systems

Recently new smart phone operating systems like Android [20] and Bada [21] have been released. Nobody knows yet how vulnerable they are going be.

D. Security solutions

Mobile devices can be protected by keeping the operating system up-to-date and by disabling interfaces that are not needed (e.g. Bluetooth). There are also a few commercial security applications available for extra protection.

VI. END-USER SECURITY

End-users can access their positioning data via the internet, and their computers are vulnerable for all the typical threats of the internet. How well their equipment is protected and maintained is fully dependent on the user. This can be a security risk for satellite tracking systems, if the attacker gains access to a hosting server using stolen user accounts.

A. Security threats

1) Viruses, worms, adware, spyware

The most common security threats for end-user are viruses, worms, adware, and spyware. These threats can open ports to the system, or they can steal user accounts directly. Usually the user does not notice anything before it is too late.

2) Phishing

Phishing [22] is a method in which attacker tries to request user accounts via email, phone, or faked web sites.

B. Security solutions

There are many commercial applications available for home users to protect their computer. Usually they are complete packages that include a firewall, virus scanner, and online protection against adware/spyware.

Being aware is a good way to be secure. Suspicious web sites and unknown download sources have to be avoided and account information has to be kept in a secure place. RFC2504 [23] contains good instructions for end-users.

VII. CONCLUSION

As discussed in this paper, the satellite tracking system is quite a complicated system from the information security point of view. It contains parts of wireless and wired communication, and it is obvious that it contains information security risks if the system is not built properly.

In any case, most security risks can be mitigated, and there are already effective security solutions available that can be applied to satellite tracking systems. Securing the satellite tracking system data path is especially important if the system is used to deliver sensitive positioning data.

REFERENCES

[1] E. Airos, R. Korhonen, T. Pulkkinen, “Satelliittipaikannusjärjestelmät” [Satellite tracking systems], PVTT, Defense Forces Technical Research Centre, Publication 12, Riihimäki: 2007. Available: http://www.mil.fi/laitokset/pvtt/satelliittipaikannus.pdf
[2] 3GPP General Packet Radio Service (GPRS) Service description Stage 2, 3GPP TS 23.060 v9.2.0
[3] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0
[4] GSM World – GSM, http://www.gsmworld.com/technology/gsm/index.htm
[5] 3GPP High Speed Circuit Switched Data (HSCSD) - Stage 2, 3GPP TS 23.034 v5.2.0
[6] GSM World - EDGE, http://www.gsmworld.com/technology/edge.htm
[7] 3GPP – UMTS, http://www.3gpp.org/article/umts
[8] 3GPP – HSPA, http://www.3gpp.org/HSPA
[9] GPRS Tunneling Protocol (GTP), 3GPP TS 29.060 v5.14.0
[10] SS7 Signaling Transport in Core Network, 3GPP TS 29.202 v5.2.0
[11] CERT/CC Denial of Service, http://www.cert.org/tech_tips/denial_of_service.html
[12] pharming.org, http://www.pharming.org/index.jsp
[13] Top 10 2007 - Cross Site Scripting – OWASP, http://www.owasp.org/index.php/Top_10_2007-A1
[14] Site Security Handbook, IETF RFC 2196,1997
[15] Standard of Good Practice for Information Security, ISF Standard, 2007
[16] The Symbian Foundation, http://www.symbian.org/
[17] Apple – iPhone – Mobile phone, http://www.apple.com/iphone/
[18] R. Mogull, “The iPhone's SMS vulnerability: What we learned”, *Macworld*, 2009, Available: http://www.macworld.com/article/142179/2009/08/iphone_sms_security.html
[19] R. McMillan, ”First IPhone Worm Spreads Rick Astley Wallpaper”, *PCWorld*, 2009, Available: http://www.pcworld.com/businesscenter/article/181697/first_iphone_worm_spreads_rick_astley_wallpaper.html
[20] Androi Open Source Project, http://source.android.com/
[21] Samsung bada open platform, http://www.bada.com/
[22] APWG internet Policy Committee, http://www.antiphishing.org/index.html
[23] Users´ Security Handbook, IETF RFC 2504,1999

Publication P[2]

P. Kämppi, J. Rajamäki, R. Guinness, Information security risks for satellite tracking systems, International Journal of Computers and Communications, Issue 1, Volume 3, 2009, ISBN: 978-5-900780-69-6, pp. 9-16.

Information security risks for satellite tracking

Pasi Kämppi, Jyri Rajamäki, Robert Guinness

***Abstract*—**Satellite tracking is one of the most rapidly growing service business areas in the world, and there are already many commercial applications available. Benefits of the service for the customer are advertised, but very seldom there is any mention of information security of the system. Modern satellite tracking systems contain communication and data processing on many levels, so they are vulnerable to many risks of information security. This paper covers the main satellite tracking system information security vulnerabilities and gives guidelines on how to make systems and services more secure.

***Keywords*—**Information security, Internet, Mobile network, Satellite tracking

I. Introduction

Satellite tracking is one of the most rapidly growing business areas in the world [1]. Tracking devices have become quite cheap, and they are available to nearly everybody. Even smart phones can be used as tracking devices.

During the last decade, mobile network coverage has also grown, and internet has become a part of our everyday life. This evolution has enabled the innovation of new solutions, and one of them is the satellite tracking system.

Risks of satellite tracking have not been investigated widely, so a few students of Laurea University of Applied Sciences started to make preliminary research in 2008, which then gave rise to the SATERISK (SATEllite tracking RISKs) research project [2]; this paper is a part of this large research project.

Preliminary research revealed that information security in satellite tracking systems is not guaranteed, and this paper describes major vulnerabilities and gives some guidelines on how information security can be improved. Further research on the risks of satellite tracking is still needed; Chapter II presents the SATERISK research project; Chapter III describes the four segments (satellite, communications, data processing and end-user segment) of satellite tracking systems; the next four chapters, Chapters IV, V, VI and VII, discuss data security risks and solutions of these four segments, and these are followed by conclusions in Chapter VII and by references.

Manuscript received January 29, 2010. This work was supported in by Laurea University of Applied Sciences, by Tekes – the Finnish Funding Agency for Technology and Innovation and by some private and governmental organizations.

P. Kämppi is with Nokia Siemens Networks, Karaportti 3, Espoo, 02610 Espoo, Finland (phone: 358-50-5140823; e-mail: pasi.p.kamppi@ laurea.fi).

R. Guinness and J. Rajamäki are with the Laurea University of Applied Sciences, Vanha Maantie 9, Espoo, 02650 Finland.

II. SATERISK Project

SATERISK is a Finnish research project, which aims at a situation where devices and services, operations procedures, as well as laws and legislations on positioning and tracking, will allow the use of so-called m2m (machine to machine) tracking devices across state and union borders.

The project aims to bring new know-how on an international level to the European security field. The project will also create new methods and development paths for positioning and tracking systems. The widely-used US-based GPS (Global Positioning System) and Russian-based GLOSNASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) satellite positioning systems will soon get an EU counterpart and rival from Galileo [3]. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. The SATERISK project also aims to offer technological solutions to issues that arise while the project is ongoing.

SATERISK is a joint research project of universities, public organizations and private companies with regard to positioning, navigation and tracking systems on the whole tracking value chain, as shown in Fig. 1, founded by the participants and by Tekes – the Finnish Funding Agency for Technology and Innovation. The aim of the project is to evaluate the technical, operational and legislative needs and the associated risks for positioning and tracking, here and now, as well as in the future. Geographical examinations areas are (1) Finland, (2) EU / the Schengen Agreement Application Convention (SAAC) area and (4) Russia.

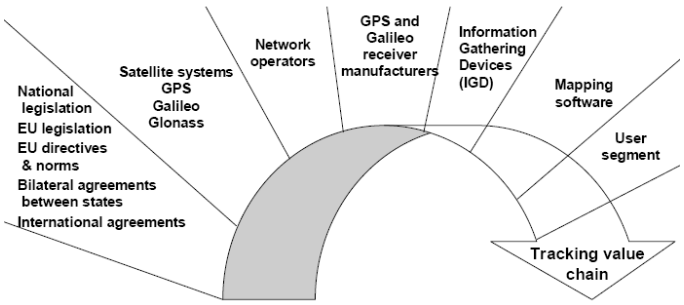


Fig. 1 Sectors of SATERISK project

Near-border and cross-border procedures for satellite tracking information, as well as the international co-

operability are studied in [4] and [5]. An example of a technical risk, jamming, is studied in [6]. This paper is one part of the research on the technical risks of satellite tracking systems, mainly studied by Laurea University of Applied Sciences.

III. Satellite Tracking Systems

Modern satellite tracking systems consist of four main technical segments: the satellite and tracking segment, communication segment, data processing segment, and end-user segment. The basic principle is that the tracked device is positioned by satellites, and the positioning data is delivered for post-processing via mobile networks and the internet. This principle is shown in Fig. 2. As an example, Fig. 3 describes the case of a remotely-tracked vehicle.

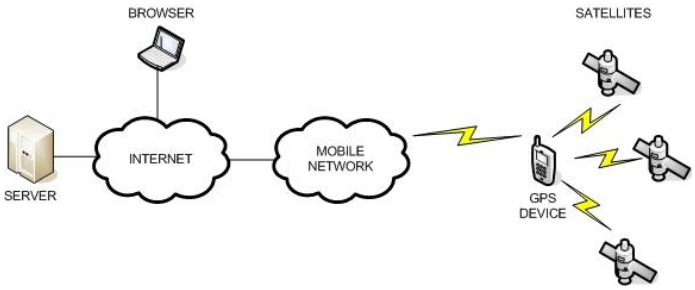


Fig. 2 Principle of a satellite tracking system [7]

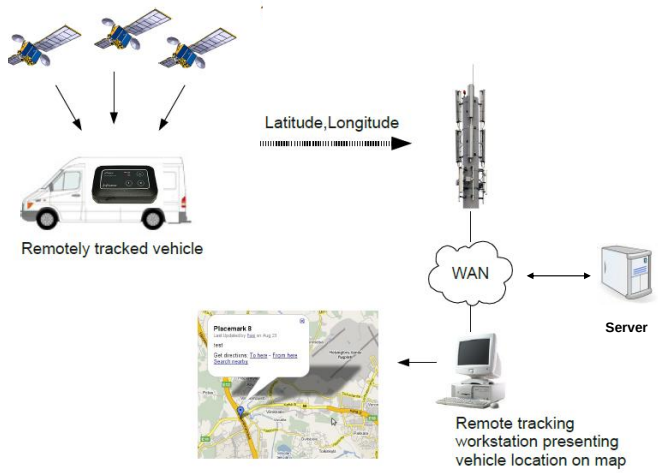


Fig. 3 Concept of remotely tracked vehicle

A. Satellite and tracking segment

The satellite and tracking segment contains satellites, radio path for satellite signals, signal receivers and techniques to calculate the device's position from satellite signals. With regard to this study, the following satellite systems are relevant.

1) GPS

The most commonly used satellite positioning system is the Global Positioning System (GPS). It has been developed by the U.S. military, but service is also available for civilian usage. The system consists of 26-28 active satellites, and it covers the whole world. Since the U.S. government stopped intentionally degrading the signal in 2000, the position data provided by GPS is quite accurate in Finland. [8]

2) GLONASS

GLONASS is developed and used by Russia. The system is like GPS, and in principle it should be able to offer as accurate as position service as GPS. In practice, the number of satellites operating in the GLONASS constellation has been quite low (8-12), so the service is not as accurate as GPS worldwide. The satellite constellation is optimized so that usability is best within Russian borders. [8]

3) GALILEO

GALILEO is under development by EGNOS (European Geostationary Navigation Overlay Service). EGNOS is a project that is sponsored by ESA (European Space Agency) and the European Commission. The goal of this project is to develop navigation services for civilian usage, independent of the military. GALILEO is technically like GPS and GLONASS, and some devices will be able to utilize all three systems. In this way, several techniques can be used simultaneously to guarantee better positioning accuracy and reliability. [8]

B. Communication segment

The communication segment contains techniques to deliver positioning data for post-processing and use by end-users. The most commonly used techniques are offered by mobile networks, namely the General Packet Radio System (GPRS) [9] and Short Message Service (SMS) [10]. The internet is used to route positioning data from mobile networks for post-processing, and this makes the system globally available. End-users can access their data via the internet as well.

C. Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data available. End-users can access their services via the internet, so systems have to be connected to the internet safely and reliably.

D. End-user segment

The end-user segment offers customer interfaces for their positioning data. Typically interfaces are offered via an internet connection and web browser.

IV. Satellite and Tracking Segment Security

Fig. 4 shows the satellite and tracking segment elements with the main technical challenges described in balloons. Commercial service providers and service users cannot contribute to the space constellation, data security of satellites

and the signals they are transmitting. Somehow, service providers and users could manage the radio path for satellite signals by operating procedures (e.g. avoid tunnels), by observations (e.g. checking possible jamming [6]) and by utilizing technical accessories (e.g. pseudolites [11], [12]). However, tracking devices are the main elements of satellite and tracking segment where service providers and user could contribute. Tracking devices might be dedicated devices or smart phones. The data security ability of dedicated tracking devices could vary significantly; some highly secure solutions are limited only to government agencies, e.g. [13]. On the other hand, data security of smart phones is highly dependent on the client software and the users' actions.

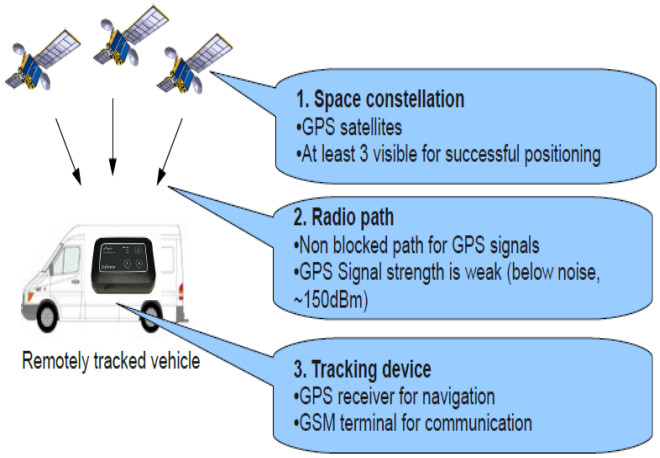


Fig. 4 Satellite and tracking segment elements

A. Client Security

Some commercial satellite tracking service providers have made matters easy by reusing smart phones as tracking devices. The user needs only to download a tracking application to turn his or her smart phone into a tracking device. Smart phones can be compared to computers in that they can have security vulnerabilities depending on the operating system used.

1) Symbian OS

Symbian is probably the most widely-used smart phone operating system in the world. Because it is like a computer operating system, it has many vulnerable interfaces [14]. Threats can occur via downloadable applications, GPRS, SMS, web browser, or email. In theory, it is possible that a mobile phone can be hijacked and managed remotely to direct positioning data to a place available to the attacker.

2) iPhone

The iPhone is a newcomer in the mobile world [15], however, there has already been a few severe security threats reported. It has been possible to capture iPhone data via SMS [16], and the first worms [17] have also been spread among iPhones.

3) Other operating systems

Recently new smart phone operating systems like Android [18] and Bada [19] have been released. Nobody knows yet how vulnerable they are going be.

B. Security solutions

Mobile devices can be protected by keeping the operating system up-to-date and by disabling interfaces that are not needed (e.g. Bluetooth). There are also a few commercial security applications available for extra protection.

V. Communication Segment Security

A. Overview of communication segment risks

The communication segment could be divided physically into mobile and fixed networks. Fig. 5 and Fig. 6 show the main technical challenges of these parts.

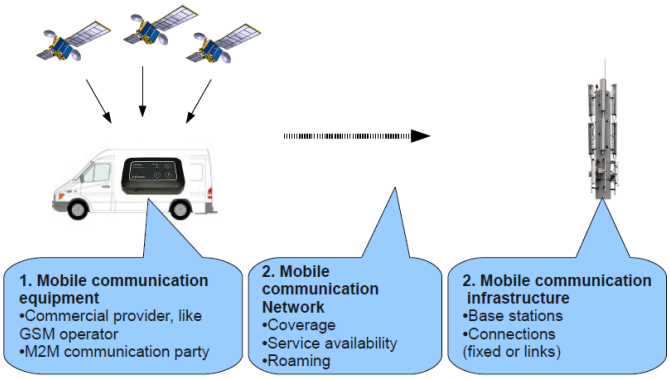


Fig. 5 Mobile communication elements

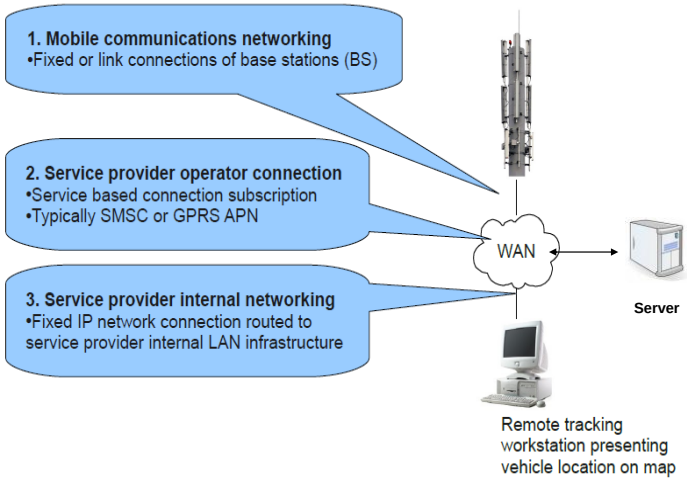


Fig. 6 Fixed network elements

B. History of mobile networks

Originally GSM (Global System for Mobile communications) [20] did not offer as advanced data services as they currently do. In the first phase, there was Circuit Switched Data (CSD), followed by High Speed Circuit Switched Data (HSCSD) [21] that offered four times faster

access rate compared to CSD. Common to these services is the use of communication channels based on a Time-Slot Leasing (TLS) sheme.

The General Packet Radio Service (GPRS) was the first packet-switched mobile network service that offered an internet-like end-user experience. In its first phase, GPRS was quite slow and network delay was large. GPRS was followed by Enhanced Data Rates for Global Evolution (EDGE) [22], and it offered faster user data rate and smaller Round Trip Time (RTT).

The Universal Mobile Telecommunications System (UMTS) [23] offers end-user data rates that make as real of a mobile internet experience as possible. Modern systems are upgraded with High Speed Downlink Packet Access (HSDPA) [24], and this type of mobile internet connection is comparable to a fixed connection in terms of data rate.

Common to all these development phases is a focus on developing faster networks, but mobile networks do not natively provide secure end-to-end user plane data transfer features.

C. GPRS

Originally GPRS was built on top of the GSM network infrastructure with a few additional network elements, and it reuses the majority of the existing network architecture. Later networks were upgraded with UMTS, and a few new network elements were introduced.

Fig 7 [9] presents the logical architecture of the modern GPRS network. Each of the boxes describes a single network element or the functional entity. The interfaces between network elements and functional entities are drawn with lines and each of the interfaces carries signaling and/or user plane data. In the user plane the most vulnerable interfaces are Gn-, Gp- and Gi-interfaces.

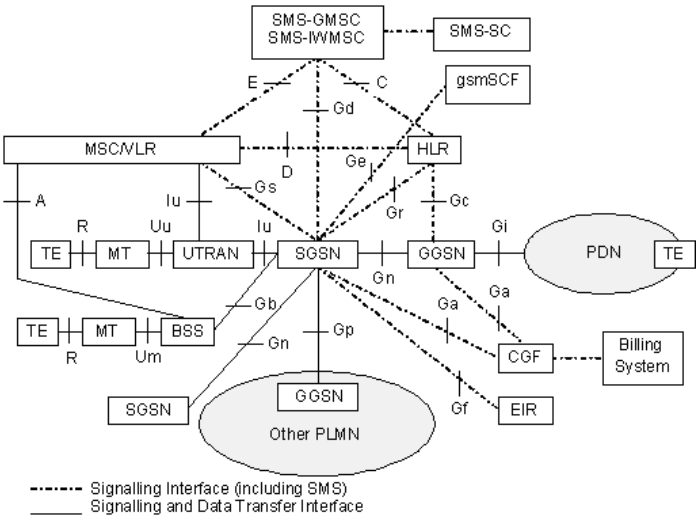


Fig. 7 GPRS Logical Architecture [9]

On the Base Sub System (BSS) and UMTS Terrestrial Radio Access Network (UTRAN), user plane data can be encrypted between Mobile Station (MS) and Service GPRS Support Node (SGSN). BSS supports the GPRS Encryption Algorithm (GEA) and UTRAN supports the UMTS Encryption Algorithm (UEA). Equipment is now available that can break ciphering from the air interface, so it is possible to capture data before it enters BSS or UTRAN.

When data continues towards a GPRS Gateway Support Node (GGSN), then data is encapsulated with GPRS Tunneling Protocol (GTP) [25] over IP. GTP does not support any encryption features. In practice, data is transferred as plain text, and it can be captured quite easily if the intruder has access to the backbone. GTP is used between operators as well, and it is quite vulnerable if traffic is routed via an insecure internet connection. From GGSN, data continues

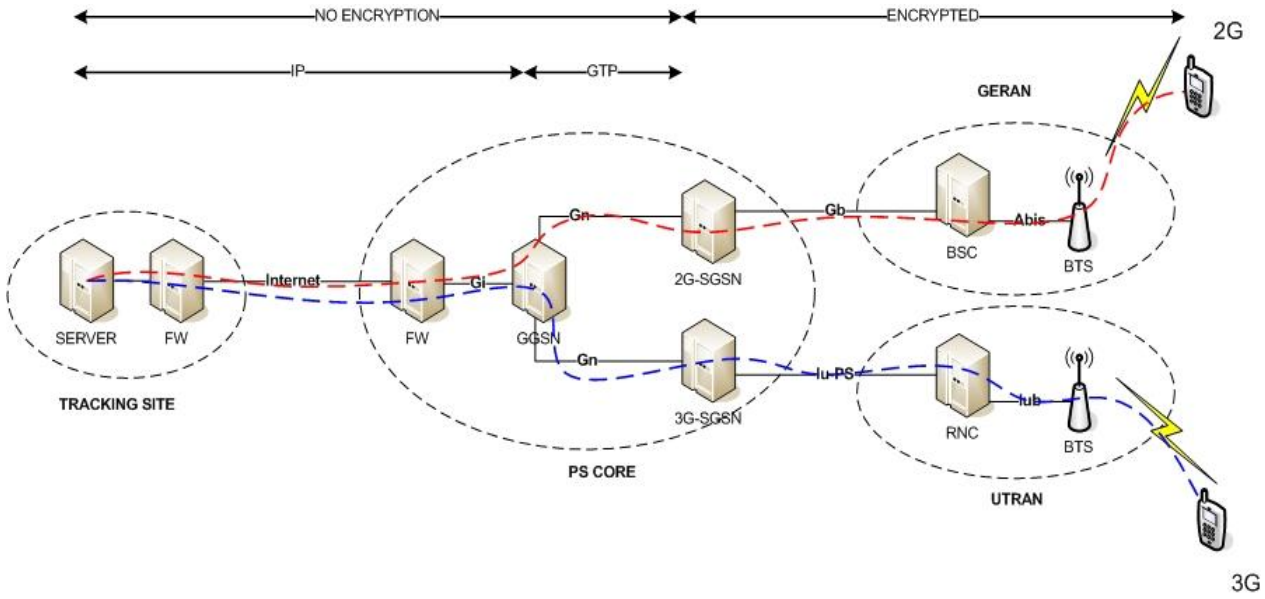


Fig. 8 Data flow in GPRS

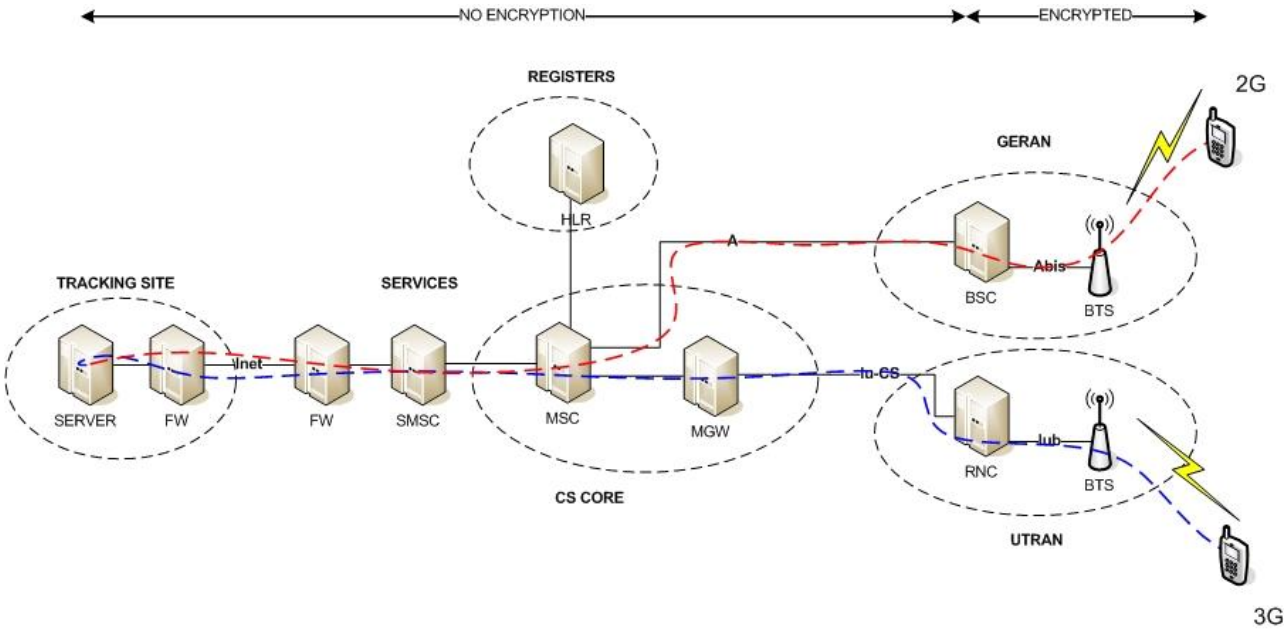


Fig. 9 Routing of SMS

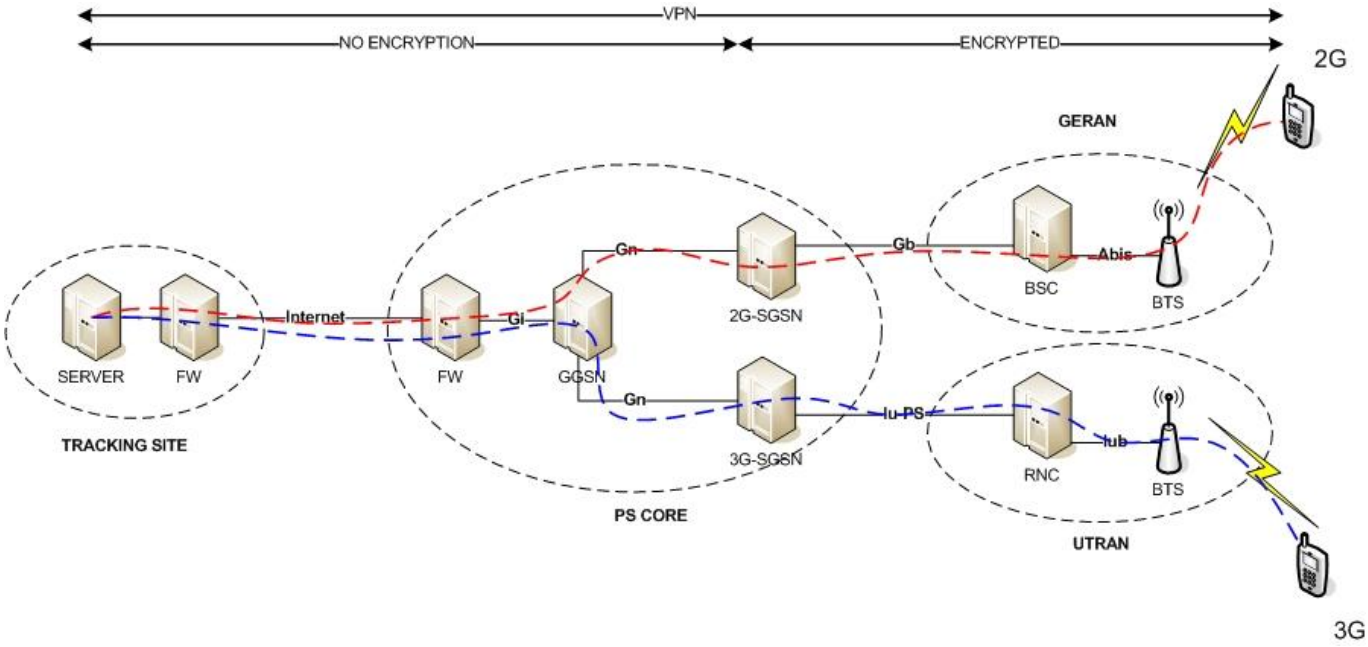


Fig. 10 GPRS security solution

towards the internet, and then data is available to anybody. Data flow is presented in Fig. 8.

D. Short Message Service

The Short Message Service (SMS) provides a method to send short messages via mobile networks [10]. Messages are delivered using signaling, and they are encrypted only in the air interface. After BSS and UTRAN they are transferred as plain text. From BSS and UTRAN the message continues towards the Mobile Switching Center (MSC) and Short Message Service Center (SMSC).

Networks of different operators are connected globally with Signaling System Seven (SS7) [26], so short messages are delivered between operators using SS7 as well. SS7 does not support any security functions, so it is possible to capture messages from the operator network if somebody is able to break in. Nowadays SS7 can be carried over IP, and this makes SS7 even more vulnerable if signaling between operators is routed via an insecure internet path. On the internet, signaling data is available to anybody.

In satellite tracking systems, positioning data is delivered for post-processing by a machine to machine (M2M) interface. Typically these interfaces (e.g. CIMD2) do not support any security functions, and data can be routed via an insecure internet path. Routing of SMS is presented in Fig. 9.

E. Security solutions

As discussed above, it is quite obvious that positioning data can not be carried safely via mobile networks. Globally there are many different operators with different information security practices, so the end-user can not rely on data being delivered safely. In the most blatant case, when data enters the internet, then it is available to anybody.

1) Data protection with GPRS

Data can be protected by establishing secure tunneling between the client and data processing center. By secure tunneling, we can make data transfer as secure as the chosen encryption method. The most common technique is IP Secure Architecture (IPsec). GPRS security solution is presented in Fig. 10.

2) Data protection with SMS

Due to the fact that SMS is delivered in mobile network signaling, it can not be secured by tunneling like GPRS data. SMS is plain text, so it can encrypted before sending by using Secure Hash Algorithms (SHA), such as SHA-256, SHA-384, or SHA-512. SMS security solution is presented in Fig. 11.

VI. Data Processing Segment Security

Position data is processed and stored in a place that can be compared to a small corporate data center from the security point of view. A data center is typically connected to the internet, so it is vulnerable for many threats like denial of service (DOS)-attacks, viruses, worms, pharming, cross scripting, and social engineering.

In some commercial satellite tracking solutions, the data center is hosted by the service provider, so the user can not be sure how positioning data is hosted. There are many open questions like: Where is the data center located, what kind of protection mechanisms are used, what is the professional level of the personnel, and is there any co-operation with government? Therefore, the user has to be aware of what service is chosen.

A. Security threats

1) Denial of service -attacks

The aim of denial of service attacks [27] is to make a website unavailable. A website can be overloaded by the attacker, and users will not be able to access their data.

2) Viruses

A computer virus is a small applet that needs a host program for spreading. Usually their purpose is to cause some harm to the infected system.

3) Worms

Worms are small applications that can spread independently in networks and execute code autonomously. Their goals are to cause disasters, open new security holes, and steal data.

4) Pharming

Pharming [28] is an attack in which a user is directed to a fake website instead of the real one. The user does not notice that they are at the fake website, so sensitive information like username and password can be stolen. Another term for this threat is “DNS cache poisoning”.

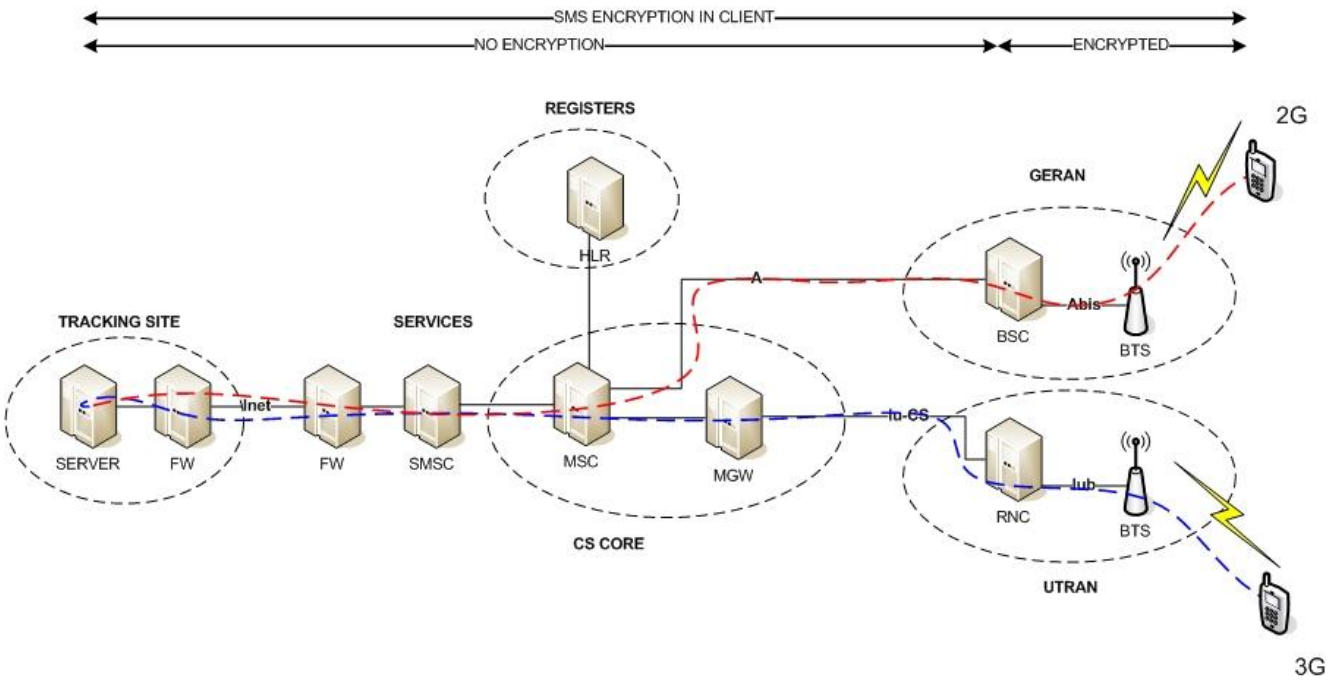


Fig. 11 SMS security solution

5) Cross site scripting

Cross site scripting (XSS) [29] is a WWW-server vulnerability where the attacker can execute code in the HTTP address or via an interactive webpage. The purpose can be to steal data or usernames.

6) Social engineering

Social engineering is a method in which somebody is tricked into giving sensitive information to the attacker. This is a very common way to discover data about a company.

B. Security solutions

There are many security threats when services are available via the internet and only a few have been introduced here. The main way service providers can protect their users is to be aware of these threats and make the system as secure as possible.

1) Best practices

There are many guides that include instructions on how to create secure networks, for example, *RFC2196 Site Security Handbook* [30] and *Standard of Good Practice for Information Security* [31].

2) Personnel

Information security is an area where knowledge has to be updated frequently. Personnel have to be aware about possible threats, which can be achieved by proper training.

3) Security equipment

Corporate networks can be secured with additional equipment like firewalls, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). A well-planned security solution is built by using all of them as needed.

4) Operating systems

It is important to keep operating system software updated. There are frequent new software releases, and maintenance personnel have to be aware of these updates. Operating systems can be "hardened," meaning that all unnecessary services are disabled.

VII. End-User Segment Security

Fig. 12 shows the main technical challenges of data processing and end-user segments. End-users can access their positioning data via the internet, and their computers are vulnerable for all the typical threats of the internet. How well their equipment is protected and maintained is fully dependent on the user. This can be a security risk for satellite tracking systems, if the attacker gains access to a hosting server using stolen user accounts.

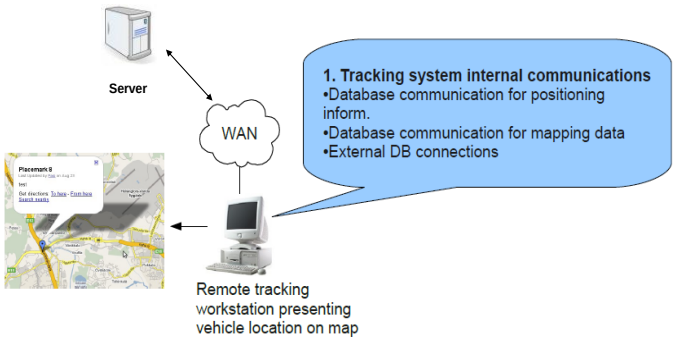


Fig. 12 Data processing and end-user segment elements

A. Security threats

1) Viruses, worms, adware, spyware

The most common security threats for end-user are viruses, worms, adware, and spyware. These threats can open ports to the system, or they can steal user accounts directly. Usually the user does not notice anything before it is too late.

2) Phishing

Phishing [32] is a method in which the attacker tries to request user accounts via email, phone, or faked web sites.

B. Security solutions

There are many commercial applications available for home users to protect their computer. Usually they are complete packages that include a firewall, virus scanner, and online protection against adware/spyware.

Being aware is a good way to be secure. Suspicious web sites and unknown download sources have to be avoided and account information has to be kept in a secure place. RFC2504 [33] contains good instructions for end-users.

VIII. Conclusion

As discussed in this paper, the satellite tracking system is quite a complicated system from the information security point of view. It contains parts of wireless and wired communication, and it is obvious that it contains information security risks if the system is not built properly. Many commercial satellite tracking applications are available, but normally no mention of their data security is given.

In any case, most security risks can be mitigated, and there are already effective security solutions available that can be applied to satellite tracking systems. Service providers and users are more likely to security precautions seriously is they are aware of the wide range of vulnerabilities. Securing the satellite tracking system data path is especially important if the system is used to deliver sensitive positioning data.

REFERENCES

[1] Viitanen, J., "Planning and requirement analysis of the SATERISK project", Master thesis, Laurea University of Applied Sciences, Espoo 2009. (In Finnish)

[2] SATERISK project, http://www.saterisk.com

[3] OPINION of the European Economic and Social Committee on the Green Paper on Satellite Navigation Applications COM(2006)769 final, Available: http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=en&docnr=989&year=2007

[4] Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. "International and Transorganizational Information Flow of Tracking Data", Proceedings of the 8th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP '09), Puerto De La Cruz, Canary Islands, Spain, December 14-16, 2009, pp. 111-115.

[5] Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. "Near Border Procedures for Tracking Information", WSEAS TRANSACTIONS ON SYSTEMS, In Press.

[6] Happonen, M., Kokkonen, P., Viitanen, J., Ojala, J. & Rajamäki, J., "Jamming Detection in the Future Navigation and Tracking Systems", in Proceedings of the 16th Saint Petersburg International Conference on Integrated Navigation Systems, 25 - 27 May, 2009 Saint Petersburg, Russia, pp. 314-317. ISBN 978-5-900780-69-6

[7] Kämppi, P., Rajamäki, J. & Guinness, R., "Information Security in Satellite Tracking Systems", Proceedings of the 3rd International Conference on Communications and Information Technology (CIT'09), Vouliagmeni Beach, Athens Greece, December 29-31, 2009, pp. 153-157.

[8] E. Airos, R. Korhonen, T. Pulkkinen, "Satelliittipaikannusjärjestelmät" [Satellite tracking systems], PVTT, Defense Forces Technical Research Centre, Publication 12, Riihimäki: 2007. Available: http://www.mil.fi/laitokset/pvtt/satelliittipaikannus.pdf

[9] 3GPP General Packet Radio Service (GPRS) Service description Stage 2, 3GPP TS 23.060 v9.2.0

[10] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0

[11] B. W. Parkinson and K. T. Fitzgibbon, "Optimal Locations of Pseudolites for Differential GPS," Navigation: The Journal of the Institute of Navigation, Vol. 33, No. 4, Winter 1986 - 87, pp. 259 - 283.

[12] B. Elrod, K. Barltrop and A. J. Van Dierendonck, "Testing of GPS Augmented with Pseudolites for Precision Approach Applications," Proceedings of ION GPS-94, 7th International Technical Meeting of The Satellite Division of the Institute of Navigation, Salt Lake City, UT, September 20 - 23, 1994, pp. 1269 - 1278.

[13] Trevoc Ltd, http://www.trevoc.com

[14] The Symbian Foundation, http://www.symbian.org/

[15] Apple – iPhone – Mobile phone, http://www.apple.com/iphone/

[16] R. Mogull, "The iPhone's SMS vulnerability: What we learned", Macworld, 2009, Available: http://www.macworld.com/article/142179/2009/08/iphone_sms_security.html

[17] R. McMillan, "First IPhone Worm Spreads Rick Astley Wallpaper", PCWorld, 2009, Available: http://www.pcworld.com/businesscenter/article/181697/first_iphone_worm_spreads_rick_astley_wallpaper.html

[18] Androi Open Source Project, http://source.android.com/

[19] Samsung bada open platform, http://www.bada.com/

[20] GSM World – GSM, http://www.gsmworld.com/technology/gsm/index.htm

[21] 3GPP High Speed Circuit Switched Data (HSCSD) - Stage 2, 3GPP TS 23.034 v5.2.0

[22] GSM World - EDGE, http://www.gsmworld.com/technology/edge.htm

[23] 3GPP – UMTS, http://www.3gpp.org/article/umts

[24] 3GPP – HSPA, http://www.3gpp.org/HSPA

[25] GPRS Tunneling Protocol (GTP), 3GPP TS 29.060 v5.14.0

[26] SS7 Signaling Transport in Core Network, 3GPP TS 29.202 v5.2.0

[27] CERT/CC Denial of Service, http://www.cert.org/tech_tips/denial_of_service.html

[28] pharming.org, http://www.pharming.org/index.jsp

[29] Top 10 2007 - Cross Site Scripting – OWASP, http://www.owasp.org/index.php/Top_10_2007-A1

[30] Site Security Handbook, IETF RFC 2196,1997

[31] Standard of Good Practice for Information Security, ISF Standard, 2007

[32] APWG Internet Policy Committee, http://www.antiphishing.org/index.html

[33] Users´ Security Handbook, IETF RFC 2504,1999

Pasi P. Kämppi was born in Varkaus, Finland on 11th December 1973. Educational background is presented in chronological order: Upper secondary school, Varkaus, Finland, 1992; B.Sc. in telecommunications, University of Applied Sciences, Kotka, Finland, 1996; Specializing studies of data network designing, Laurea University of Applied Sciences, Espoo, Finland, 2009.

He performed his military service on 1996-1997 and he was ranked as sergeant in signal corps. He has been working with telecommunications since 1997. He started his career on 1997 in Nokia Networks as Testing Engineer and then he has been working as Senior Testing Engineer and System Specialist. Currently he is working as Senior System Specialist in Nokia Siemens Networks. His special interest is packet switched mobile networks including IP networks. He started his MBA program in Laurea University of Applied Sciences at the beginning of 2010 and this paper is part of his Master's Thesis.

Jyri K. Rajamäki was born in Punkalaidun, Finland 1963. He received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea's Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored more than 40 scientific publications.

Dr. Rajamäki has been an active actor in the field of electrotechnical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM. He is currently the Scientific Manager of two Tekes projects.

Robert Guinness was born in St. Louis, Missouri, USA in 1981. He received his B.A. in physics from Washington University in St. Louis in 2004 and his M.Sc. in space studies from the International Space University (ISU) in Strasbourg, France in 2006. He conducted his thesis research at Johnson Space Center in Houston, Texas, where he completed a conceptual design of a crewed lunar lander.

In 1998 he completed a Missouri Space Grant Consortium internship in the Remote Sensing Laboratory at Washington University in St. Louis, conducting research on dust accumulation on Mars using data from the Mars Viking missions. From 2000 to 2004 he was a researcher in the Laboratory for Space Sciences at Washington University, conducting chemical and isotopic measurements of meteorite samples to study presolar grains. In 2001, he completed the NASA Academy at Goddard Space Flight Center, where he analyzed data from the Keck Observatory on circumstellar dust clouds. In 2002, he was a guest researcher at the Max Planck Institute for Chemistry in Mainz, Germany, where he conducted further research on presolar grains. From 2006 to 2008, he worked for Hamilton Sundstrand as a Mission Support Scientist and Lead Increment Scientist Representative for the International Space (ISS) program. Since 2008 he has worked for the Boeing Company and served as an Increment Payload Engineer for the ISS program, where he was responsible for the mission integration of 130 experiments conducted during Expeditions 19 and 20. Since 2009, he is also Director of Aerospace Systems for American Pioneer Ventures, a firm dedicated to helping early-stage startups and entrepreneurs achieve success. In December 2009, he came to Laurea University of Applied Sciences as a guest researcher, where he has participated in the SATERISK and Mayfly projects.

Mr. Guinness is a member of the Space Generation Advisory Council (SGAC) and served as the Regional Coordinator for the North and Central America and Caribbean region from 2006 to 2009.

Publication P[3]

P. Kämppi, R. Guinness, Technical Risk Analysis for Satellite Based Tracking Systems, Integrated Communications Navigation and Surveillance Conference, Herndon, VA, USA, May 2010, ISBN: 978-1-4244-7457-8, pp. M3-1 – M3-16.

TECHNICAL RISK ANALYSIS FOR SATELLITE BASED TRACKING SYSTEMS

Pasi Kämppi, Laurea University of Applied Sciences, Espoo, Finland
Robert Guinness, Laurea University of Applied Sciences, Espoo, Finland

Abstract

Satellite tracking is one of the most rapidly growing business areas in the world [1], and there are already many commercial applications available like fleet management [2] or equipment theft alert [3]. Service providers advertise benefits for the customer, but they rarely mention the technical risks inherent in a tracking system. Modern satellite tracking systems require communication and functionality on many levels, so they are vulnerable to many technical risks. This paper describes system overview of satellite-based tracking, several risk analysis methods, covers the main technical risks of a satellite tracking system, and demonstrates usage of the developed risk analysis tool.

Introduction

Satellite tracking is one of the most rapidly growing business areas in the world [1]. Tracking devices have become relatively inexpensive [4], [5], and they are widely available on the commercial market. Even smart phones can be used as tracking devices.

In addition, mobile network coverage has grown rapidly during the last decade, and mobile telecommunication has become a part of our everyday lives. This evolution has enabled the innovation of new services, such as satellite-based tracking applications.

The technical risks of satellite tracking have not been thoroughly investigated, so there is a need to determine how to make satellite-based tracking applications operate. Many times service providers only advertise the benefits of their applications with no warnings about the risks inherent in these systems.

Satellite tracking system contains functionality on many levels, and it is difficult to perform risk analysis that covers every technical threat that exists. The first part of this paper explains how the tracking system operates and covers the most vulnerable parts of the satellite tracking system.

The second part reviews several methods of risk analysis, including qualitative risk analysis and grounded theory. The third part describes how we used grounded theory to identify risks of satellite-based tracking. The fourth part elaborates these technical risks in more detail. In the fifth part, we describe the risk analysis tool that we developed during this research. The sixth part presents three risk analysis cases that were analyzed with this tool. The last part contains discussion of the results and conclusions.

System Overview of Satellite-based Tracking

Modern satellite-based tracking systems consists of many technical segments, including the satellite segment, user segment, communication segment, data processing segment and end-user segment. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS), and positioning data is delivered for post-processing via mobile networks, the internet or a secure network. The principle is portrayed in figure 1.

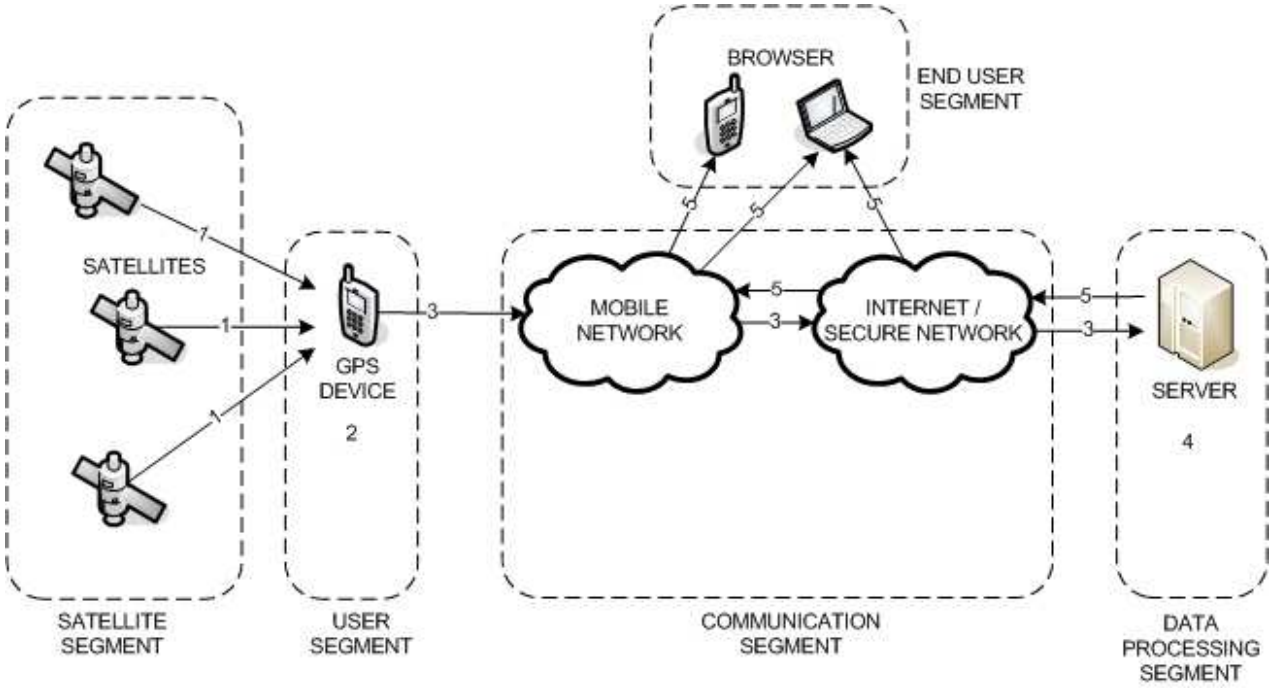


Figure 1. Satellite tracking system

1. Satellite segment

The satellite segment contains systems to deliver signals for calculating position.

GPS (Global Positioning System) is the most commonly used satellite positioning system [6]. It has been developed by the U.S. Department of Defense (DoD), but service has been offered for civilian usage as well. The system contains 26-31 active satellites [7], and it covers almost the entire world. The position determined by GPS is accurate to about 10-20m, since the government stopped intentionally degrading the signal for civilian usage in 2000.

GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) [8] was developed and is maintained and used by the Russian government. The system is similar to GPS, and it should be able to offer a position service as accurate as GPS. The satellite constellation has improved during late years and the current system contains 21-23 active satellites [9].

Galileo [10] is under development by the European Tripartite Group (ETG), which is made up of the European Community (EC), Eurocontrol, and the European Space Agency (ESA). The first phase of Galileo is the European Geostationary Navigation Overlay Service (EGNOS) project, which will provide a Satellite-Based Augmentation System (SBAS) to improve the accuracy of GPS and GLONASS within Europe and its neighboring regions. The overall objective of the Galileo program, however, is to develop an independent navigation service for civilian usage with better performance than the current GPS service. Galileo is technically similar to GPS and GLONASS.

COMPASS/Beidou [11] is under development by China Satellite Navigation Project Center (CSNPC). The target of the project is to have full satellite constellation (35 satellites) by year 2020. The first satellite was launched on 17th January 2010.

2. User segment

The user segment contains devices that are able to calculate and deliver position information for post processing. Today many mobile phones include GPS receivers, and it is easy to turn a mobile phone into a tracking device [12]. For

professional services and public authorities, TETRA clients [13] and tracking-only clients (without communications functionality) are available. New positioning devices will support three systems (GPS, GLONASS, and Galileo) so that several techniques can be used simultaneously to guarantee better positioning accuracy and availability.

3. Communication segment

The communication segment contains systems to deliver positioning data for post-processing and use by end-users.

General Packet Radio System (GPRS) [14] is an extension of the Global System for Mobile Communications (GSM), and it offers mobile packet switched access. GSM offers connectivity in more than 218 countries and covers more than 80% of the world's population [15]. The data rate offered is 40-300 kbit/s, and round trip time (RTT) is up to few seconds. Global network coverage is presented in figure 2 [16].

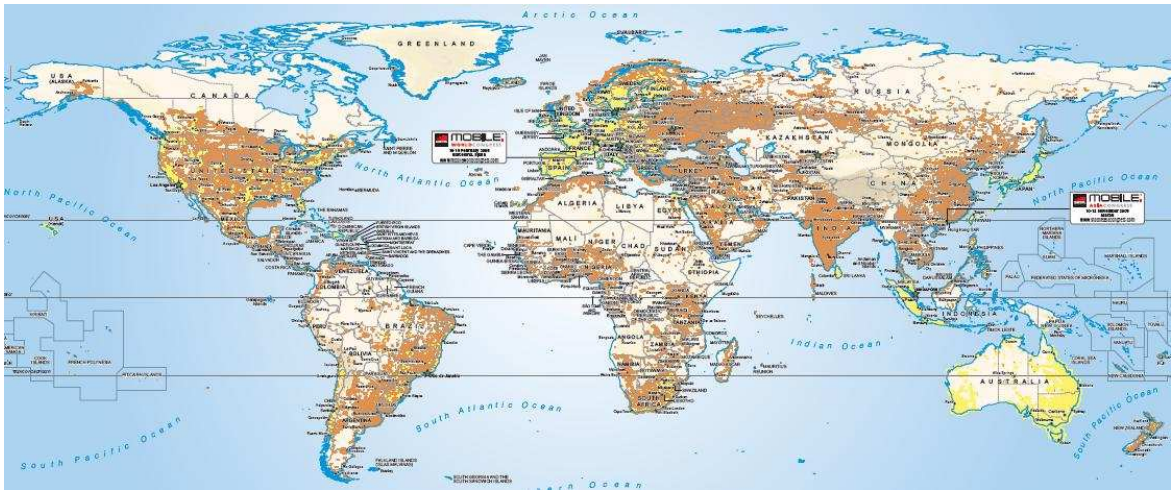


Figure 2. GSM and UMTS network coverage

Universal Mobile Telecommunications System (UMTS) [17] is the successor to GSM. It offers voice, messaging and data services. The data rate is higher and RTT is shorter compared to GSM. The data rate offered is up to 14 Mbit/s [18]. Radio coverage is continually expanding, and UMTS covers the most populated areas.

Short Message Service (SMS) [19] is the messaging service of GSM and UMTS. It allows users to send and receive text messages on a mobile phone. The length of the messages is 160 characters, and messages can be sent globally via different operators.

Long Term Evolution (LTE) [20] is fourth-generation (4G) telecommunication standard. LTE offers a packet-optimized service without native support for voice communication. The data rate offered is up to 300 Mbit/s [20] with low RTT. The first commercial networks were launched in Scandinavia in late 2009.

Terrestrial Trunked Radio (TETRA) [21] is developed for the professional services like police and fire departments. It offers voice, short data and packet data services. Strong security features and dedicated capacity are essential for professional use. The latest release of TETRA offers data rates up to 500 kbit/s [22].

Worldwide Interoperability for Microwave Access (WiMAX) [23] is based on open 802.16 standards. WiMAX offers a packet-switched service, and voice communication is not supported. Data rates are up to 75 Mbit/s. WiMAX is currently deployed in 147 countries, and 620 million people are covered [24].

4. Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data usable for end-users. End-users can access their services via the Internet or a secured network. Systems have to be connected to the Internet safely and reliably. Secured networks are used for the professional services.

5. End-user segment

The end-user segment offers customer interfaces for their positioning data. Typically the interface is offered via a network connection and web browser. Mobile terminals can be used as customer interfaces, too.

Use cases under study

Before performing any risk analysis, it is important to know how a system will be used. Particularly for complicated systems, such as satellite-based tracking, it is difficult if not impossible to understand the risks involved in the system in a generic way. By choosing a diverse set of use cases, however, one can consider a wide set of risks. As the number and diversity of the use cases under study grows, the risks inherent in the system can be known in a quasi-generic manner.

In the current research, we chose five dissimilar use cases, based on current or proposed uses of satellite-based tracking. These use cases are described briefly below.

Road toll

EU directive 2004/52/EC [25] is the driving force for the EU wide road toll system in the Europe. The tax is based on driven kilometers, time of the day and used route. Netherlands is the first country that has decided to deploy location based road toll [26]. Road toll sets high requirements for the whole system.

The number of the cars is high and number of the transaction is high too. The location data is not allowed to be lost because the tax is based on tracking. And the finally, tracking device has to work in the demanding environment of the car.

Fleet management

Satellite tracking can be used for fleet management to track cars, trucks, trailers and containers [2]. The fleet is possible to locate with tracking system and time schedules can be planned optimally. Stolen or missing fleet can be located more easily too.

Fleet management requires wide network coverage and sets high standards for the tracking device. Trucks and containers are moving around the world and the tracking devices are installed in various environments.

Traffic light management

The traffic light management for public transportation is deployed in Helsinki, Finland [27]. When a bus is coming into traffic lights the green light is lit on as soon as possible.

System requires low network latency and dedicated capacity because the traffic lights are managed in real time.

Rescue department and security service

Rescue department uses location information for managing troops via centralized system [28]. Head quarters have real time information about position of the troops and they can give new instructions based on location information.

Operations are executed in very demanding environmental circumstances and that requires high quality tracking devices [29].

Cash In Transit

The cash in transit is tracked in real time [30]. If the tracked target leaves the route or disappears from the map then there is probable security threat.

Cash in transit tracking is one the most demanding tracking solutions. It requires high data privacy, ability for the real time tracking and possibility for intentional interference is existent.

Risk analysis methods

Introduction to risk analysis

The purpose of risk analysis is not to eliminate all risks because this is rarely possible. Risk analysis is used to find out the most severe risks, and reduce these risks to an acceptable level.

For example, in the business of securely transporting money, there may be many methods available for mitigating risks, but each has an associated cost. The company must determine if the risk mitigation is worth the cost. The company may be aware of many risks, but only the most harmful ones will be mitigated with cost-effective safeguards.

In this research, we focused on creating a flexible model to determine the most severe risks satellite-based tracking systems. The model can be used to evaluate real business cases several examples of which will be described below. First, however, we will briefly review the major methods of risk analysis.

Quantitative risk analysis

The target of quantitative risk analysis is to define a monetary or other numerical value for potential losses [31] and determine the probabilities that such losses will occur for a given set of operations. It is often based on historical data, and the probability of a threat occurring is calculated by complex procedures.

Quantitative risk analysis is appropriate for frequently-occurring phenomenon, but it is particularly challenging when used to detect threats that are known but have never occurred [32].

Qualitative risk analysis

The target of qualitative risk analysis is to define subjective definitions for potential losses and their associated likelihood of occurring [31]. Of the severity and likelihood of potential losses can be described with terms like low, medium and high.

Qualitative risk analysis can describe very rare threats or threats that have not been measured with quantitative risk analysis. Qualitative risk analysis can provide useful results but only if the risk management team is competent and can assess the risks accurately.

Process for qualitative risk analysis

The target of this research was to find out the most severe risks and analyze them in a flexible way, so the qualitative risk analysis was selected. It is easy to learn, it is very flexible, and it does not require capital investments for specialized software.

We chose to use Peltier's Qualitative Risk Analysis (QRA) methodology [33]. The phases of the process are presented below.

Develop a scope statement

The risk analysis process starts with defining the scope. The scope of the risk analysis has to be clear, and the boundaries have to be set properly. If the scope is unclear, then it is possible that the results will be unreliable due to them being improperly used.

Form a competent team

In qualitative risk analysis, the risk factors are rated subjectively by a risk analysis team. It is very important that the members of the team are competent and qualified because the results are highly dependent on the competence of the team.

Identify assets

An asset is something that has value [34]. The asset can be tangible or intangible. Tangible assets include items that can be seen or touched. Common examples of tangible assets include a machine or furniture. Intangible assets include more abstract entities like data or information.

Identify threats

The risk analysis team defines the threats that are under review. If there is no existing list of threats, then the list can be made by brainstorming. Each member of the team writes down notes, and then notes are combined into a more complete list. If an existing list of threats is available, then the list can be reviewed and improved if needed. The drawback with this method is that it can limit thinking. The team members may look only at the existing list, and this may not foster new ideas. Finally, the list of threats should be properly categorized.

Prioritize threats

When the threats are defined, then the risk analysis process can continue by prioritizing risks. In practice, prioritizing means defining subjective value for the probability of the threat to occur. This probability is defined subjectively from low to high, and it is expressed as a numerical value, as defined in Table 1. If the evaluation is made independently by each team member, then the total threat priority is calculated as the average of the values assigned. When prioritizing the threats, it is important to keep a strong focus in the case that is under study. In other words, the team must estimate what the probability is of the threat in the case that is under study.

Table 2 present total threat prioritizing.

Table 1. Priority table

Low	Low to Medium	Medium	Medium To High	High
1	2	3	4	5

Table 2 present total threat prioritizing.

Table 2. Total threat priority

Threat	Priority
Threat 1	3
Threat 2	2
Threat 3	2
Threat 4	3

Impact priority

In this phase, the team evaluates the impact of the loss occurring, again using the scale shown in Table 1. If the evaluation is made independently by each team member, then the final loss impact is calculated as the average. There has to be some discussion after the evaluations, and ideally each team member should be satisfied with the results. Threat impact evaluations are presented in Table 3.

Table 3.Total loss impact

Threat	Priority	Loss impact
Threat 1	3	5
Threat 2	2	5
Threat 3	2	3
Threat 4	3	5

Calculate total threat impact

The total timpact of a threat can be defined as a risk factor, too. The risk factor is calculated as the sum of the threat priority and loss impact. The risk factor range is from 2 to 10. Calculation of the risk factor is presented in Table 4.

Table 4. Risk factor calculation

Threat	Priority	Loss impact	Risk factor
Threat 1	3	5	8
Threat 2	2	5	7
Threat 3	2	3	5
Threat 4	3	5	8

After risk factor calculation, the table is sorted by risk factors to find out the most severe threats.

Grounded Theory as a tool for risk analysis

The risk analysis method we used does not offer tools or guidelines for categorizing threats, so we used Grounded Theory.

Grounded Theory offers methodology to categorize data and to investigate relations between categories. The method encourages moving from the particular to the more general thinking [35].

Grounded Theory is not widely used in information systems research but there are few cases where grounded theory has been combined with other research methods [36].

Next chapter describes how we used Grounded Theory with risk analysis.

Identifying threats of satellite-based tracking

In order to avoid the problem of limited existing data or limited knowledge of the risk analysis team, it is necessary to investigate the requirements of the applications and businesses, too. An application can have technical requirements that have not been levied on prior uses of the system. If the system can not offer service with certain requirements, then it is a threat for the application. The requirements of the business can create technical requirements, and the technical limitations of the system causes threats to those requirements being met. Using this approach, we were able to generate a model for identifying threats, shown in Figure 3.

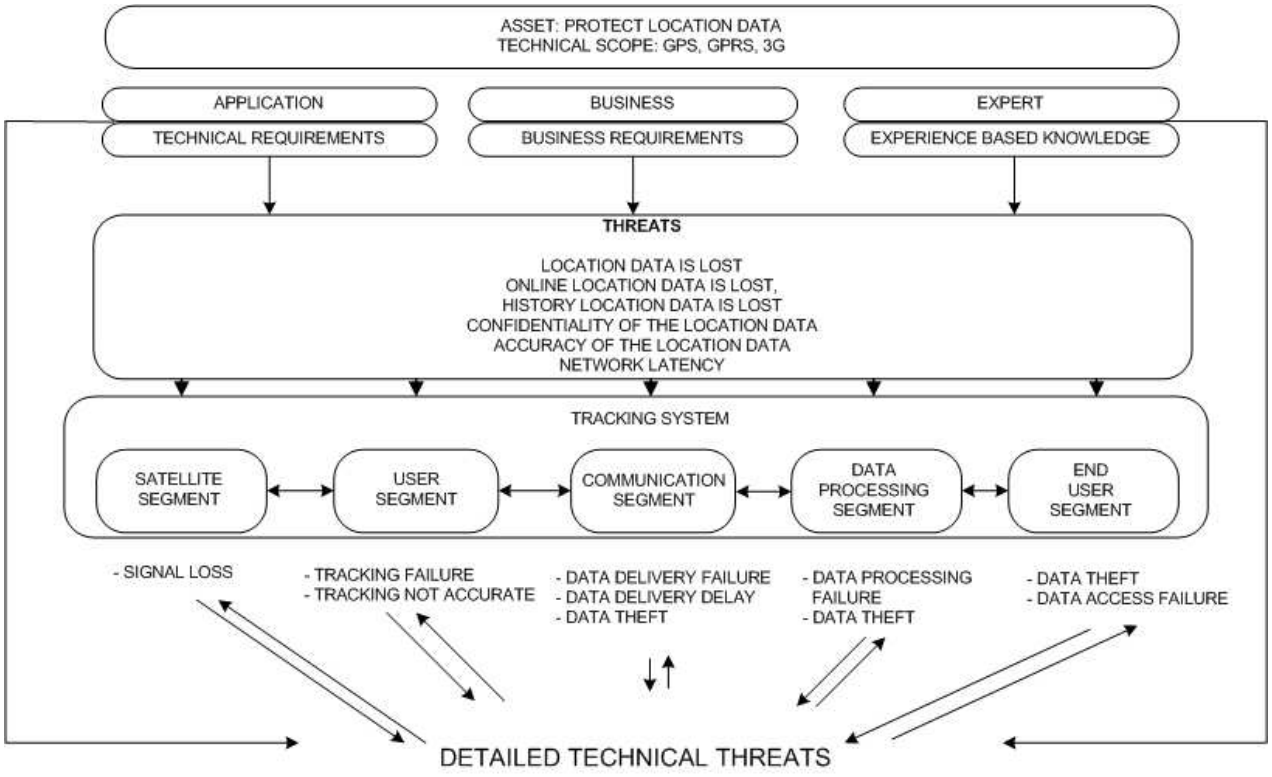


Figure 3. Model for identifying technical threats

We started identifying threats by listing well known technical threats. Our scope was limited to cover GPS, GPRS, 3G and SMS because the expertise of our risk analysis team was primarily in these areas. The asset we chose to investigate was location data.

First, we defined the segments of the system and groups threats according to the segments in which they occur.

We discovered that a single technical threat can be the cause for some higher-level threat. For example, the cause of a tracking failure can be a technical problem in tracking device. The technical problem is the lower-level threat, and the tracking failure is the higher-level threat.

Also, we noticed that higher-level threats can help to find lower level threats. Data privacy threats are caused by certain technical reasons. The data privacy is higher level threat and the technical reason is the lower level threat.

Next, we investigated if higher-level threat could occur in the other segments of the system. For example, privacy threats can be caused by many technical reasons in many segments. This cycle generated relations between all threats and segments.

When we had sorted all well known threats we added requirements of the use cases described before.

The results of this methodology are described below with the threats grouped by system segment and category

Detailed description of the threats

This section gives a more detailed description of technical threats that were discovered. Threats are grouped by segment and logical category.

Satellite segment

Unintended interference

Unintended interference can be caused by other radio transmitters that are working nearby the frequencies used by the positioning satellites (L1=1547,42 MHz , L2=1227,60 MHz) [6]. Weakly shielded or faulty electronics can cause interference, too.

Intentional interference

Intentional interference can be caused by sending interfering signals on the same frequency band that the satellite systems are using. Equipment that is used to generate interfering signals is called a jammer. GPS-jammers are quite easily available via the Internet, and they are inexpensive [37]. Prices for portable devices are starting from around $30, and the effective range is 2-300m.

Atmospheric conditions

The ionosphere and troposphere can cause variation of the speed of the GPS signal. Speed variation can cause 0-30m errors [38].

Multipath propagation

Multipath propagation occurs when the signal is reflected from surrounding elements like buildings. Multipath propagation can cause 1 meter error [38].

Selective availability

The Department of Defense can make intentional alteration of the time and epherimis signal, called Selective Availability (SA). SA can cause 0-70m errors [38]. SA was stopped on May 2000.

Total signal loss

Total signal loss can occur when contact with the satellites is lost. These situations can occur in tunnels or parking garages.

User Segment

HW fault

Hardware faults can occur due to environmental variables or other causes. Typical causes are mechanical stress, temperature change, high humidity, and aging.

SW fault

Software faults can occur in the operating system or in applications. SW errors can cause processing errors, data output errors or processing delays.

Power feed breakdown

The power feed for a tracking device can be external power source or internal batteries. Power feed breakdown can halt use of the tracking device completely.

Clock drift

The internal clock of the GPS receiver is not precise compared to atomic clocks onboard the satellites. Clock drift can cause 0-1.5m error [38].

Signal attenuation / Measurement noise

Signal attenuation can occur if the tracking device is installed improperly or there are mechanical faults in antenna lines. Signal attenuation can cause 0-10m error [38].

Information security

It is theoretically possible to hijack a smart phone and steal data. There has been vulnerabilities found for the iPhone [39] and Android [40]. This is a potential risk in the future.

Communication segment

Mobile phone intentional interference

Intentional interference can be caused by sending interfering signals on the same frequency band than radio network is using. Equipment that is used to generate interfering signals is called a jammer. Mobile phone jammers are quite easily available via the internet, and they are inexpensive [41]. Multifunctional devices can generate interference for radio network frequencies and GPS.

Prices for portable devices start at around $30, and the effective range is 2-20m.

GPRS capacity

GPRS user plane capacity could be a problem in highly populated areas. Rapidly growing use of mobile internet causes stress for mobile networks. Rural areas could have very limited GPRS capacity, or there may not be GPRS capacity at all. High amount of mobility requires network signaling capacity.

GPRS latency

Round-trip time (RTT) in GPRS can vary a lot, and it can be greater than 1000ms.

GPRS information security

GPRS offers data encryption only on the radio interface. Data is delivered without encryption in the core network [42]. Data flow on the user plane is presented in Figure 4.

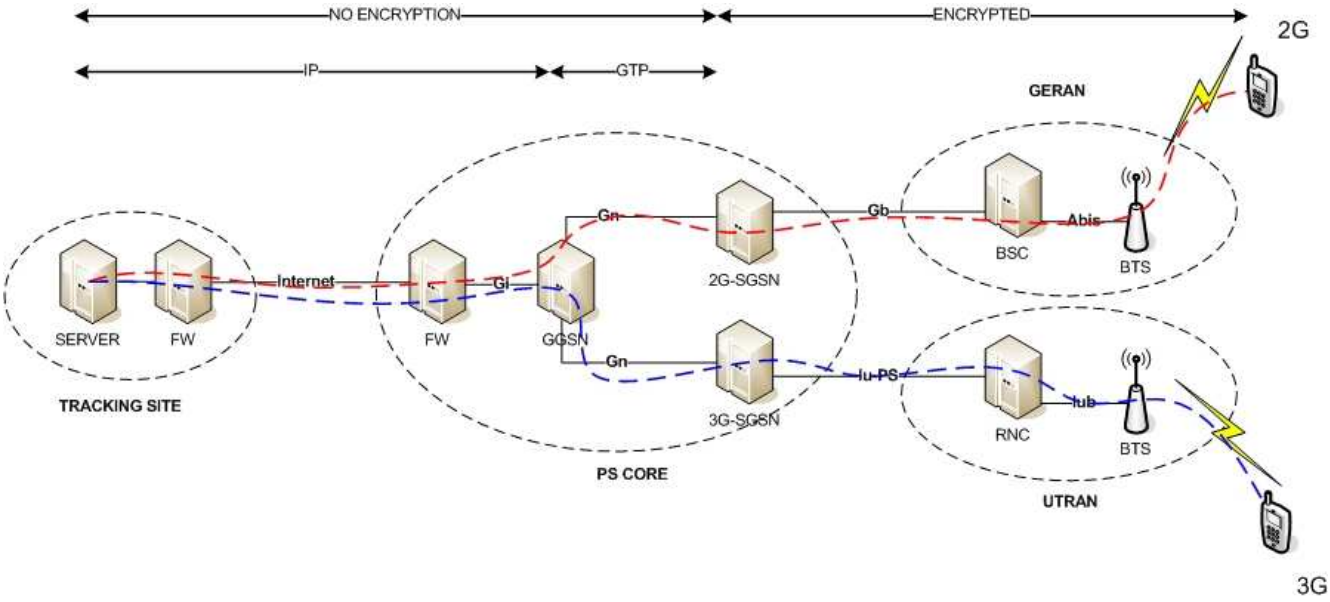


Figure 4. Data flow in GPRS and UMTS

GPRS radio coverage

Although GSM offers connectivity in more than 218 countries and covers more that 80% of the world's population, [15] there are still areas that are not covered by GSM [16], including parts of Canada, South America, Africa, Russia and Australia. Europe is well covered with GSM.

GPRS roaming

Roaming is the situation when a device is moving outside of its home network [43]. Roaming can cause a situation when the mobile device is not able to deliver location data via GPRS.

3G packet data capacity

3G offers higher data rates and more capacity than GSM, but use is increasing due to the real mobile Internet experience that it provides. Networks can run out of capacity in highly populated areas, and there has already been cases reported of capacity problems [44]. High amounts of mobility require high network signaling capacity.

3G packet data latency

3G offers much lower RTT compared to GSM. RTT is typically 200-300 ms.

3G information security

GPRS offers data encryption only on the radio interface. Data is delivered without encryption in the core network [42]. Data flow on the user plane for 3G is also presented above in Figure 4.

3G radio coverage

3G has good radio coverage in North, West and South Europe. Other parts of the world are expanding their networks [16].

3G roaming

Roaming is the situation when a device is moving outside of home network [43]. Roaming can cause situation when the mobile is not able to deliver location data via packet switched services.

SMS capacity

SMS is delivered in signaling. SMS delivery does not reserve radio network user plane capacity like GPRS or normal speech. Capacity is dependent on the operator.

SMS latency

Delivery time of the SMS can be even 10 seconds [45], depending on operator and location. If SMS is not delivered at first try, then it is buffered by the network for resending.

SMS information security

Delivery of the SMS is encrypted only in the radio network. SMS is delivered without encryption in the core network and even between operators [42], Figure 5.

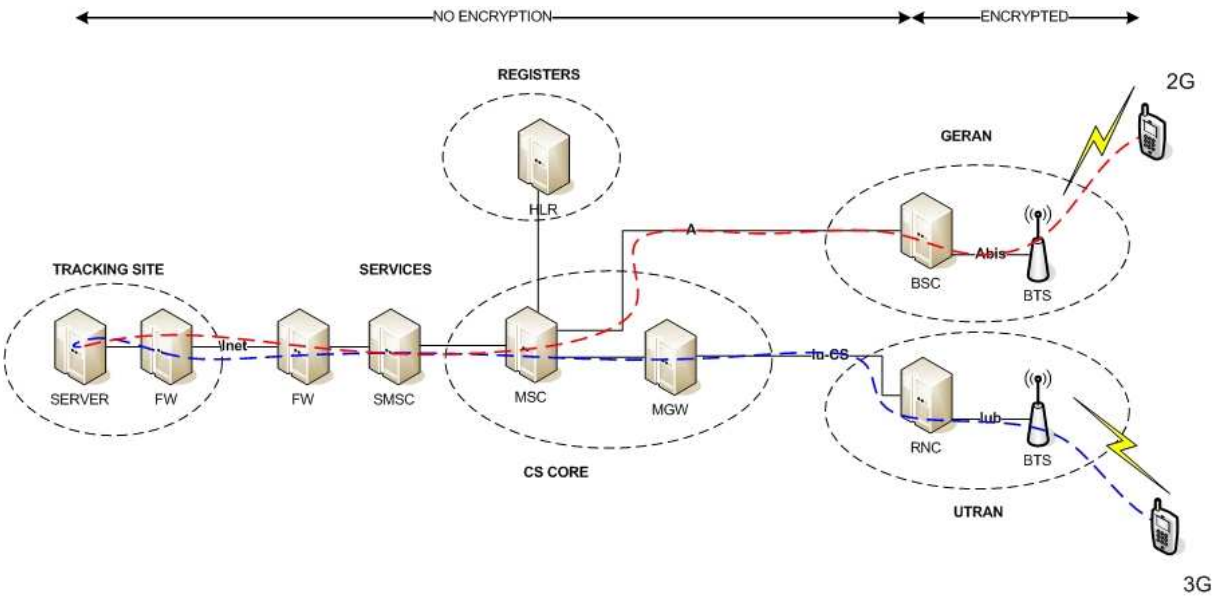


Figure 5. Delivery of the SMS

Internet capacity

Capacity depends on used access network capacity, core network capacity and current network load.

Internet latency

Delivery time of the data depends on the capacity of the access network being used, as well as the current network load and distance between delivery points.

Internet information security

Data is not encrypted as default when delivered via Internet. Unsecured and sensitive data can be potential target for the hackers.

Data processing segment

HW fault

Hardware faults can occur by environmental variables. Typical variables are mechanical stress, temperature changes, great humidity and aging.

SW fault

SW fault can occur in operating system or in application. SW error can cause processing errors, data output errors or processing delays.

Power feed breakdown

Power source failure can cause partial or total service outage.

Processing capacity

The large number of the transactions in some applications requires significant processing

capacity. Lack of capacity can cause system malfunction.

Information security

Location data is delivered and accessed via external networks. The data center where the information is stored has to be protected properly against external security threats (virus, DOS-attack, etc).

Database corruption

Database corruption can cause loss of history data. Database corruption can be caused by e.g. hard disk failure or electricity break.

End user segment

Information security

The location information can be accessed with a computer or mobile client, depending on the application. Possible vulnerabilities are weak password, weak virus protection and unshielded internet connection.

Risk analysis tool

When all technical threats were defined, we then decided to implement an Excel-based tool for risk analysis. Excel is easy to use, and it offers a flexible platform.

We defined six questions for impact prioritizing:

- How critical is it for the business that location data is determined and recorded at all times?
- How critical is it for the business that real-time location data is known and delivered to the end-user, or is buffering allowed?
- How critical is it for the business that the historcal position data is stored and maintained?
- What are the needs for confidentiality of the data?
- How important is network latency?
- How important is location accuracy?

Description of the risk analysis tool

The risk analysis was recorded using Excel-based spreadsheets. The spreadsheets include columns for country, index, segments, threats, probabilities, loss impact and total risk factors. Each threat was inserted in the chart and sorted by system segment. The threat probabilities were evaluated separately for each threat. A loss impact could have relations with many technical threats, and they were evaluated with questions that we defined earlier. The loss impact values were copied automatically into the same row from related threats. The risk factors were calculated automatically as the sum of the threat probabilities and loss impacts. The risk analysis tool is presented in Figure 6.

					FILL ME			
	HOV CRITICAL IS FOR THE BUSINESS THAT LOCATION DATA IS LOST							
	HOV CRITICAL IS FOR THE BUSINESS THAT REAL TIME LOCATION DATA IS LOST (buffering allowed)							
	HOV CRITICAL IS FOR THE BUSINESS THAT HISTORY DATA IS LOST							
	WHAT IS CONFIDENTIALITY OF THE LOCATION DATA							
	REQUIREMENTS FOR NETWORK LATENCY							
	REQUIREMENTS FOR LOCATION ACCURACY							
	COUNTRY	INDEX	CATEGORY	THREAT	THREAT OCCURE	LOSS	THREAT LOSS IMPACT	RISK FACTOR
		1	SATELLITE SEGMENT	GPS - UNINTENDED INTERFERENCE		NO LOCATION DATA	0	0
		1	SATELLITE SEGMENT	GPS - INTENTIONAL INTERFERENCE		NO LOCATION DATA	0	0
		1	SATELLITE SEGMENT	GPS - ATMOSPHERIC CONDITIONS		ACCURACY	0	0
		1	SATELLITE SEGMENT	GPS - MULTIPATH PROPAGATION		ACCURACY	0	0
		1	SATELLITE SEGMENT	GPS - SELECTIVE AVAILABILITY		ACCURACY	0	0
		1	SATELLITE SEGMENT	GPS - TOTAL SIGNAL LOSS		NO LOCATION DATA	0	0
		1	SATELLITE SEGMENT	GPS - THEORETICAL ACCURACY		ACCURACY	0	0
		2	USER SEGMENT	DEVICE - HW-FAULTS		NO LOCATION DATA	0	0
		2	USER SEGMENT	DEVICE - SW-FAULTS		NO LOCATION DATA	0	0
		2	USER SEGMENT	DEVICE - POWER FEED BREAKDOWN		NO LOCATION DATA	0	0
		2	USER SEGMENT	DEVICE - CLOCK DRIFT		ACCURACY	0	0
		2	USER SEGMENT	DEVICE - SIGNAL ATTENUATION / MEASUREMENT NOISE		ACCURACY	0	0
		2	USER SEGMENT	DEVICE - MOBILE PHONE INFORMATION SECURITY		DATA CONFIDENTIALITY	0	0
		3	COMMUNICATION SEGMENT	GPRS - CAPACITY		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	GPRS - LATENCY		LATENCY	0	0
		3	COMMUNICATION SEGMENT	GPRS - ENCRYPTION		DATA CONFIDENTIALITY	0	0
		3	COMMUNICATION SEGMENT	GPRS - RADIO COVERAGE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	GPRS - ROAMING		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	GPRS - UNINTENDED INTERFERENCE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	GPRS - INTENTIONAL INTERFERENCE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	3G - PACKET DATA CAPACITY		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	3G - PACKET DATA LATENCY		LATENCY	0	0
		3	COMMUNICATION SEGMENT	3G - RADIO COVERAGE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	3G - ROAMING		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	3G - ENCRYPTION		DATA CONFIDENTIALITY	0	0
		3	COMMUNICATION SEGMENT	3G - UNINTENDED INTERFERENCE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	3G - INTENTIONAL INTERFERENCE		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	SMS - CAPACITY		NO REAL TIME LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	SMS - LATENCY		LATENCY	0	0
		3	COMMUNICATION SEGMENT	SMS - ENCRYPTION		DATA CONFIDENTIALITY	0	0
		3	COMMUNICATION SEGMENT	INTERNET - CAPACITY		NO LOCATION DATA	0	0
		3	COMMUNICATION SEGMENT	INTERNET - DELAY		LATENCY	0	0
		3	COMMUNICATION SEGMENT	INTERNET - ENCRYPTION		DATA CONFIDENTIALITY	0	0
		4	DATA PROCESSING SEGMENT	HW-FAULTS		NO LOCATION DATA	0	0
		4	DATA PROCESSING SEGMENT	SW-FAULTS		NO LOCATION DATA	0	0
		4	DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN		NO LOCATION DATA	0	0
		4	DATA PROCESSING SEGMENT	INFORMATION SECURITY		DATA CONFIDENTIALITY	0	0
		4	DATA PROCESSING SEGMENT	DATABASE CORRUPTION		HISTORY DATA LOST	0	0
		4	DATA PROCESSING SEGMENT	PROCESSING CAPACITY		NO LOCATION DATA	0	0
		5	END USER SEGMENT	HOME USER - INFORMATION SECURITY		DATA CONFIDENTIALITY	0	0
		5	END USER SEGMENT	PROFESSIONAL USER - INFORMATION SECURITY		DATA CONFIDENTIALITY	0	0

Figure 6. Risk analysis tool

Risk analysis cases

Of the five use cases described above, we chose three for initial testing of our methodology and tool. The first two are existing uses of satellite-based tracking, and thus, our results could conceivably be compared to real-world data, if available. The third is a fictional use case, but it could be tested via simulation. The use cases and result are presented below.

Personal Fitness and Sporting Activities

Satellite tracking can be used to track personal fitness activities like jogging. We installed tracking client software into a smart phone and created a user account on a free service that we found on the Internet. There is no relation of this use case to any business case, but it is an easily implemented example of using satellite-based tracking. Listed below are key characteristics of this use case, applicable to risk analysis:

- Activity: Jogging
- Geographic Area: Espoo, Finland
- Service provider: gpsgate.com [46]
- Smart phone: Nokia N95
- Application: GSM Tracker [12]
- Positioning System: GPS
- Communication System: GPRS / 3G

CATEGORY	THREAT	RISK FACTOR
DATA PROCESSING SEGMENT	HW-FAULTS	6
DATA PROCESSING SEGMENT	SW-FAULTS	6
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	6
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	6
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	6
USER SEGMENT	GPS - TOTAL SIGNAL LOSS	5
USER SEGMENT	DEVICE - HW-FAULTS	5
USER SEGMENT	DEVICE - SW-FAULTS	5
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	5
COMMUNICATION SEGMENT	INTERNET - CAPACITY	5
END USER SEGMENT	HOME USER - INFORMATION SECURITY	5

Figure 7. Jogging risk profile

After analyzing this use case, we evaluated the overall risk profile as medium. The most critical threats are found from the data processing and tracking segments.

Road toll Netherlands

As described above, Netherlands has decided to deploy road toll system that is based on driven kilometers [26]. The system will cover whole Netherlands, and people are charged whenever they are driving a car. The location data is very crucial for the business, and location data must not be lost in any circumstances. The tracking device is able to buffer data if network connection is lost. It is possible that some people are using jammers to avoid road tolls.

Listed below are key characteristics of this use case:

- Activity: Automobile driving
- Geographic area: Netherlands (entire country)
- Extent of coverage: 137000 km of roadway
- Number of tracking devices: 8 million cars
- Tracking Device: On Board Unit (OBU)
- Data Buffering: Supported by OBU Positioning System: currently GPS Galileo proposed for the future
- Communication System: GPRS

CATEGORY	THREAT	RISK FACTOR
USER SEGMENT	GPS - UNINTENDED INTERFERENCE	8
SATELLITE SEGMENT	GPS - INTENTIONAL INTERFERENCE	8
USER SEGMENT	DEVICE - HW-FAULTS	8
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	8
COMMUNICATION SEGMENT	INTERNET - CAPACITY	8
COMMUNICATION SEGMENT	INTERNET - ENCRYPTION	8
DATA PROCESSING SEGMENT	HW-FAULTS	8
DATA PROCESSING SEGMENT	SW-FAULTS	8
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	8
DATA PROCESSING SEGMENT	INFORMATION SECURITY	8
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	8
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	8
END USER SEGMENT	HOME USER - INFORMATION SECURITY	8
END USER SEGMENT	PROFESSIONAL USER - INFORMATION SECURITY	8
SATELLITE SEGMENT	GPS - TOTAL SIGNAL LOSS	7
USER SEGMENT	DEVICE - SW-FAULTS	7
COMMUNICATION SEGMENT	GPRS - CAPACITY	7
COMMUNICATION SEGMENT	GPRS - ENCRYPTION	7
COMMUNICATION SEGMENT	GPRS - RADIO COVERAGE	6
COMMUNICATION SEGMENT	GPRS - ROAMING	6

Figure 8. Road toll risk profile

The overall risk profile for this use case was evaluated to be from medium to high. The usage of intentional interference could be fatal for the system, and this particular risk is rated high on the scale. Problems with the tracking device could cause loss of location data. The road tax is based on the data collected, and any problems in data processing could lead to unreliable billing.

Tracking of the Cash In Transit

Cash in transit can be tracked with a satellite-based tracking system. In a fictional case, cash in transit is tracked in the Helsinki capital area. Robbery is possible [47], and many criminals might be using jammers. Location data is very sensitive, and real-time tracking is mandatory.

Below are listed available facts for risk analysis:

- Activity: Cash In Transit
- Geographic Area: Helsinki capital area
- Tracking Device: Dedicated tracking device
- Positioning System: GPS
- Communication System: GPRS / 3G
- Additional Threat: Usage of the jammers possible

CATEGORY	THREAT	RISK FACTOR
SATELLITE SEGMENT	GPS - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	GPRS - ENCRYPTION	9
COMMUNICATION SEGMENT	GPRS - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	3G - ENCRYPTION	9
COMMUNICATION SEGMENT	3G - INTENTIONAL INTERFERENCE	9
COMMUNICATION SEGMENT	INTERNET - ENCRYPTION	9
DATA PROCESSING SEGMENT	INFORMATION SECURITY	9
END USER SEGMENT	HOME USER - INFORMATION SECURITY	9
END USER SEGMENT	PROFESSIONAL USER - INFORMATION SECURITY	9
SATELLITE SEGMENT	GPS - TOTAL SIGNAL LOSS	8
DATA PROCESSING SEGMENT	HW-FAULTS	8
DATA PROCESSING SEGMENT	SW-FAULTS	8
DATA PROCESSING SEGMENT	POWER FEED BREAKDOWN	8
DATA PROCESSING SEGMENT	PROCESSING CAPACITY	8
USER SEGMENT	DEVICE - HW-FAULTS	7
USER SEGMENT	DEVICE - SW-FAULTS	7
USER SEGMENT	DEVICE - POWER FEED BREAKDOWN	7
COMMUNICATION SEGMENT	GPRS - CAPACITY	7
COMMUNICATION SEGMENT	3G - PACKET DATA CAPACITY	7
COMMUNICATION SEGMENT	INTERNET - CAPACITY	7
DATA PROCESSING SEGMENT	DATABASE CORRUPTION	7

Figure 9. Cash in transit risk profile

The overall risk profile of this use case was rated from medium to high. We can see that the tool can be used to highlight the high risk of intentional interference and security threats for sensitive location data.

Discussion and Conclusion

System-level risk analysis is a very complicated and demanding task, especially for complex systems. The risk analysis team has to know the basic functionality of the system, but this alone is not enough. We noticed that the risk analysis team has to be able to combine the requirements of the applications and business to the risk analysis process as well. Integrating the requirements of the applications and business with the risk analysis process helps to ensure that the scope is clear and the results are reliable.

Our tool and use cases revealed that it is not possible to make general risk profiling at the system level because different solutions have different technical requirements. The same technical threats can have different risk factor in different cases. Too

general of a risk analysis will give inaccurate results.

The model used to develop the tool described in this paper is very flexible. It is easy to add new navigation or telecommunications techniques to cover future needs. Replacing our Excell-based tool with a database-based tool could be more useful in future larger-scale research.

Grounded theory is not widely used in Information Security research. This research shows that Grounded Theory can be combined with other methodologies with great results. Grounded Theory helps the team to understand complex systems and helps the team to look at the risk profile from a new view.

Laurea University of Applied Sciences will continue studying satellite-based tracking solutions. This research is a good starting point for other students or anybody else who is interested on satellite-based tracking systems.

References

[1] EGNOS, Business support, 2009, Strategy study 2009, http://www.egnos-portal.eu/index.cfm?objectid=5B3A0970-BE43-11DE-9ECC0013D3D65949

[2] Satcom Technology, Tracking solutions, Fleet management service, http://www.satcomtechnology.com/tracking-solutions/fleet-management

[3] GpsGate.com, Solutions, Equipment Theft Alert service, http://www.gpsgate.com/index.php?id=235

[4] DigiNetLink.com, Globalsat TR-102 tracking device, http://www.diginetlink.com/GlobalSat_TR_102_Personal_Tracking_p/tr-102.htm

[5] VisiRun, Fleet tracking service, http://www.visirun.com/index.php/en?gclid=CJnIzcTe-6ACFQm7ZwodMAOswQ

[6] InsideGNSS, About GPS, http://www.insidegnss.com/aboutgps

[7] Russian Space Agency, GPS constellation status, http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:30:3625031152673081::NO

[8] InsideGNSS, About GLONASS, http://www.insidegnss.com/aboutglonass

[9] Russian Space Agency, GLONASS constellation status, http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:20:3378292882897440::NO

[10] InsideGNSS, About Galileo, http://www.insidegnss.com/aboutgalileo

[11] InsideGNSS, About COMPASS, http://www.insidegnss.com/aboutcompass

[12] Aspicore, GSM Tracker application, http://www.aspicore.com/en/tuotteet_tracker.asp

[13] Motorola, MTM800E TETRA mobile, http://www.motorola.com/Business/XU-EN/Product+Lines/Dimetra+TETRA/TETRA+Terminals/TETRA+Mobile+Radios/MTM800_Enhanced_XU-EN_PK-EN_XF-EN_XN-EN_XC-EN_XM-EN_XE-EN

[14] 3GPP, GPRS, http://www.3gpp.org/article/gprs-edge

[15] GSM World, GSM, http://www.gsmworld.com/technology/gsm/index.htm

[16] GSM World, 2009, GSM WorldPoster2009a, http://www.gsmworld.com/roaming/GSM_WorldPoster2009A.pdf

[17] 3GPP, UMTS, http://www.3gpp.org/article/umts

[18] 3GPP, HSPA, http://www.3gpp.org/HSPA

[19] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0

[20] 3GPP, LTE, http://www.3gpp.org/LTE

[21] TETRA MoU Association, http://www.tetramou.com/tetramou.aspx?id=44

[22} TETRA MoU Associaton, TETRA Release 2, http://www.tetramou.com/tetramou.aspx?&id=1186

[23] WiMAX.com, What is WiMAX, http://www.wimax.com/education

[24] WiMAX FORUM, 2010, Monthly Industry Report, http://www.wimaxforum.org/resources/monthly-industry-report

[25] European Union Law, 2004, Directive 2004/52/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:166:0124:0143:EN:PDF

[26] Ministry of Transport, Public Works and Water Management, Road Pricing, http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/road_pricing/the_basis_of_the_kilometre_price/

[27] City of Helsinki, Urban Traffic Control Center, HeLMI description, http://www.hel2.fi/liikenteenohjaus/eng/pt_telematics.asp

[28] www.gpsreview.com, 2005, Florida Fire Department uses GPS Technologu to Dispatch Vehicles, http://www.gpsreview.net/florida-fire-department-uses-gps-technology-to-dispatch-vehicles/

[29] Sandler Larry, 2009, Firefighters work trough GPS tracking problems, The Milwaukee Journal Sentinel, http://www.firerescue1.com/fire-products/apparatus-accessories/articles/603422-Wis-firefighters-work-through-GPS-tracking-problems/

[30] ASSA ABLOY, Securing valuables in transit: GPS meet biometrics, http://www.assaabloydoorsolutions.co.uk/risk/innovations/securing-valuables-in-transit-gps-meets-biometrics

[31] Peltier, Thomas R, 2001, Information Security Risk Analysis, CRC Press LLC Ltd, pp. 20-22

[32] Sainsbury, Robert, Richard Baskerville, 2007,, Possible Analysis Engine: A prototype Tool for Managing IT Security Safeguards Acquisition, Forthcoming in The International Conference on Information Warfare and Security, California

[33] Peltier, Thomas R, 2001, Information Security Risk Analysis, CRC Press LLC Ltd, pp. 23-34

[34] Peltier, Thomas R, 2001, Information Security Risk Analysis, CRC Press LLC Ltd, pp. 6-7

[35] Bryant Anthony, Kathy Charmaz, 2007, The SAGE Handbook of Grounded Theory, SAGE Publications Ltd, pp 14-17

[36] Bryant Anthony, Kathy Charmaz, 2007, The SAGE Handbook of Grounded Theory, SAGE Publications Ltd, pp 339-355

[37] Jammer World, GPS Jammer, http://www.thejammerworld.com/product_GPS_Jammer_GPS_Jammer_page_1.html

[38] Cmtinc.com, Gpsbook, Chapter Six: The GPS Error Budget, http://www.cmtinc.com/gpsbook/index.htm

[39] Mogull Rich, 2009, The iPhone's SMS Vulnerability, MacWorld, http://www.macworld.com/article/142179/2009/08/iphone_sms_security.html

[40] Sadun Erica, 2009, Android security vulnerability discovered, Ars Technica, http://arstechnica.com/open-source/news/2009/02/android-security-vulnerability-discovered.ars

[41] Jammer World, Mobile Phone Jammer, http://www.thejammerworld.com/product_Mobile_Phone_Jammer__page_1.html

[42] Kämppi, Pasi, Jyri Rajamäki, Robert Guinness, 2009, Information security in satellite tracking systems, 3rd International Conference on Communication and Information Technology, Athens, pp. 153-157

[43] GSM World, Mobile SMS and Data Roaming Explained, http://www.gsmworld.com/documents/sms_data_roaming_explained.pdf

[44] Sarno David, Los Angeles Times, 2009, http://articles.latimes.com/2009/dec/10/business/la-fi-iphone10-2009dec10

[45] ANACOM, SMS delivery time, http://www.anacom.pt/render.jsp?categoryId=167302

[46] GpsGate.com, Products, BuddyTracker, http://www.gpsgate.com/index.php?id=56

[47] Bank of Finland, 2007, Bank of Finland currency distribution function, http://www.bof.fi/en/suomen_pankki/ajankohtaista/tiedotteet/2007/tiedote8_2007.htm

2010 Integrated Communications Navigation and Surveillance (ICNS) Conference
May 11-13, 2010

Publication P[4]

P. Kämppi, R. Guinness, T. Urpila, Field Testing for Satellite Based Tracking Systems, 61st International Astronautical Congress, Prague, Czech Republic, Sep 2010, CD-ROM, 15 pages.

IAC-10-B2.1.12

FIELD TESTING FOR SATELLITE BASED TRACKING SYSTEMS

P. Kämppi
Laurea University of Applied Sciences, Finland, pasi.p.kamppi@laurea.fi

R. Guinness
Laurea University of Applied Sciences, Finland, robert.guinness@laurea.fi

T. Urpila
Laurea University of Applied Sciences, Finland, tatu.urpila@laurea.fi

Satellite-based tracking is a rapidly growing business area in many parts of the world. Tracking devices have become inexpensive, mobile network coverage has grown, and the internet has become part of our everyday life. This evolution has enabled the proliferation of satellite-based tracking applications. The basic principle behind satellite-based tracking is that a tracked device is positioned by GNSS satellites, and the positioning data is delivered for post-processing via mobile networks and the internet. This system is complex, and field testing provides an effective way to test system reliability and performance with real applications. In this research, analysis was performed on the reliability and accuracy of satellite-based tracking using commercially-available systems during various routes in several regions in Finland. A smart phone was transformed into tracking device by installing a tracking application. Data created in the mobile device was sent over mobile networks to the third-party GPS tracking service. Later data from both the GPS tracking server and the mobile phone were downloaded and analyzed. Use cases included different activities like car driving, sailing and bicycling. We found that the system performs very well and basic functionality is very stable. Practical testing, however, did reveal that the smart phone is not able to perform as well as a dedicated GPS receiver. Also, we discovered that the position of the GPS module in the mobile device greatly affects the sensitivity, and in certain models, this sensitivity changes based on whether the keyboard is exposed because the GPS module is directly beneath the keyboard. Lastly, we found a few security vulnerabilities that have not been found in theoretical risk analysis. This study describes the main structure of the satellite-based tracking system, presents known technical risks, describes the test setup we used, and gives results on the performance of the satellite-based tracking system.

I. INTRODUCTION

As the number and commonness of satellite-based tracking applications increases, the need for a comprehensive study of the safety and reliability of these services becomes more important. By *safety* we refer primarily to the information security aspects of the location data pathway, although the accuracy and availability of the location data can also have safety implications, depending on the application under consideration. *Reliability* refers to primarily to the ability of the system to perform its intended functions whenever such functions are desired, within some measureable parameters.

Considering the entire system of systems required to effectively provide satellite-based tracking services, the level of complexity is high, and the number of factors that can affect the services is large, making an end-to-end reliability evaluation challenging. The purpose of the current study, which falls under the umbrella of the long-term Saterisk project, is to measure the performance of a commercially-available mobile device tracking service under several real-world case scenarios.

II. SYSTEM OVERVIEW OF SATELLITE BASED TRACKING

Modern satellite-based tracking systems consists of many technical segments, including the control segment, space segment, user segment, communication segment, data processing segment, application interface for external applications and end-user segment. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS), and positioning data is delivered for post-processing via mobile networks, the internet or a secure network. The principle is portrayed in figure 1.

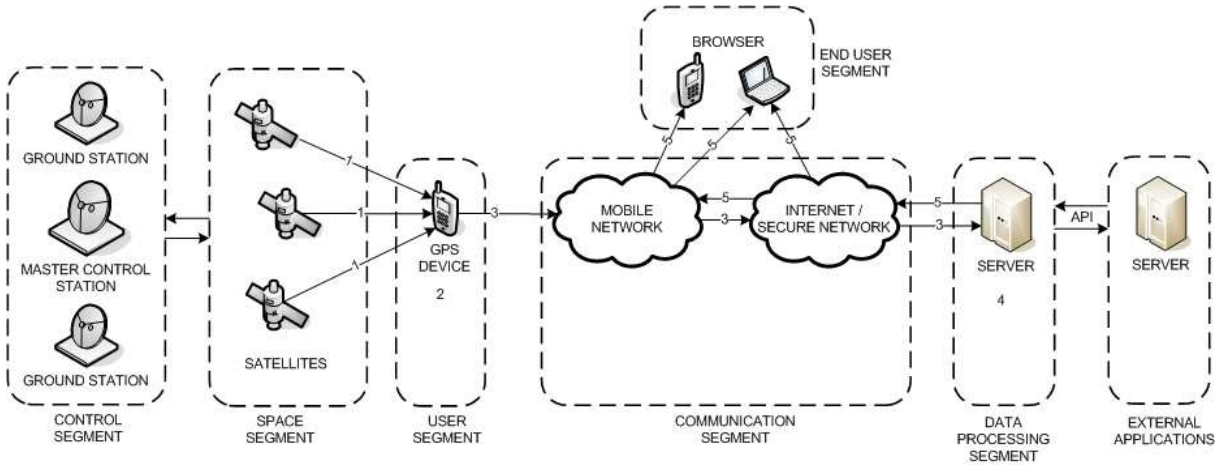


Fig. 1: Principle of the satellite based tracking system

II.I Control segment

The control segment contains master control station and ground stations that monitor satellites in space segment. Monitoring is made 24 hours in day.

Ground stations receive monitoring data from satellites and they forward data to the master control station. The master control station analyses monitoring data and sends adjustment commands to the satellites via ground stations.

II.II Space segment

The space segment contains systems to deliver signals for calculating position.

GPS (Global Positioning System)[1] is the most commonly used satellite positioning system at the moment. Even though the GPS system is being developed and operated by the United States Air Force for the Department of Defence, it is available for civilian use all over the world as well. The system currently contains 31 active satellites and it covers almost the entire world. Replacing old satellites has experienced some delays, but the new generation of satellites now being sent to the orbit will be carrying new technology to ensure reliability[2]. The position determined by the GPS system is accurate to about 10-20m, since the U.S. government stopped intentionally degrading the signal for civilian use in 2000.

GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System)[3] was developed and is maintained by the Russian government. The satellite constellation of the system has improved during the past few years containing 21-23 active satellites at the moment[4]. The system is similar to the GPS and it should be able to offer as good accuracy as the GPS system. Compatibility with other GNSS systems is possible and at the moment further developed.

Galileo[5] is under development by the European Tripartite Group (ETG), which is made up of the European Community (EC), Eurocontrol, and the European Space Agency (ESA). The first phase of Galileo is the European Geostationary Navigation Overlay Service (EGNOS) project, which will provide a Satellite-Based Augmentation System (SBAS) to improve the accuracy of GPS and GLONASS within Europe and its neighbouring regions. The overall objective of the Galileo program, however, is to develop an independent navigation service for civilian usage with better performance than the current GPS service. Galileo is technically similar to GPS and GLONASS. The full constellation will contain 30 satellites in the future.

Compass[6] is under development by China Satellite Navigation Project Center (CSNPC). China is planning to have a 12 satellites constellation, providing regional coverage, in operation in 2012. The full 35 satellites constellation is aimed to be complete in 2020 as the funding is already assured. The first satellite was launched in January 2010 and after the launch of the fifth satellite on August 1st 2010, the project is on course to completing its targets[7].

II.III User segment

The user segment contains devices that are able to calculate and deliver position information for post processing. Today many mobile phones include GPS receivers, and it is easy to turn a mobile phone into a tracking device[8]. For professional services and public authorities, TETRA clients[9] and tracking-only clients (without communications functionality) are available. New positioning devices will support three systems (GPS, GLONASS, and Galileo) so that several techniques can be used simultaneously to guarantee better positioning accuracy and availability.

II.IV Communication segment

The communication segment contains systems to deliver positioning data for post-processing and use by end-users.

General Packet Radio System (GPRS)[10] is an extension of the Global System for Mobile Communications (GSM), and it offers mobile packet switched access. GSM offers connectivity in more than 218 countries and covers more than 80% of the world's population[11]. The data rate offered is 40-300 kbit/s, and round trip time (RTT) is up to few seconds. Global network coverage is presented in figure 2[12].

Universal Mobile Telecommunications System (UMTS)[13] is the successor to GSM. It offers voice, messaging and data services. The data rate is higher and RTT is shorter compared to GSM. The data rate offered is up to 14 Mbit/s[14]. Radio coverage is continually expanding, and UMTS covers the most populated areas.

Short Message Service (SMS)[15] is the messaging service of GSM and UMTS. It allows users to send and receive text messages on a mobile phone. The length of the messages is 160 characters, and messages can be sent globally via different operators.

Long Term Evolution (LTE)[16] is fourth-generation (4G) telecommunication standard. LTE offers a packet-optimized service without native support for voice communication. The data rate offered is up to 300 Mbit/s[16] with low RTT. The first commercial networks were launched in Scandinavia in late 2009.

Terrestrial Trunked Radio (TETRA)[17] is developed for the professional services like police and fire departments. It offers voice, short data and packet data services. Strong security features and dedicated capacity are essential for professional use. The latest release of TETRA offers data rates up to 500 kbit/s[18].

Worldwide Interoperability for Microwave Access (WiMAX)[19] is based on open 802.16 standards. WiMAX offers a packet-switched service, and voice communication is not supported. Data rates are up to 75 Mbit/s. WiMAX is currently deployed in 147 countries, and 620 million people are covered[20].

II.V Data processing segment

The data processing segment contains systems to process and store position data for end-users. These systems include servers and applications that make position data usable for end-users. End-users can access their services via the Internet or a secured network. Systems have to be connected to the Internet safely and reliably. Secured networks are used for the professional services.

II.VI Application programming interface for external applications

API (Application Programming Interface)[21] allows a software program to interact with other software and operating systems. API makes it possible to combine the location data that we have acquired with other applications. Using API would also make it possible for us to do our own program that could use the data we have acquired and stored with the applications we have used. For example GpsGate service, that we have used in our research, offers API so that users can send data to and receive data from the GpsGate-service to be processed with other applications[22].

II.VII End user segment

The end-user segment offers customer interfaces for their positioning data. Typically the interface is offered via a network connection and web browser. Mobile terminals can be used as customer interfaces, too.

III. KNOWN TECHNICAL RISKS

Technical risk analysis[23] was made earlier during Saterisk project. Results of technical risk analysis give guidelines for field testing too.

III.I Control segment

As the control segment is operated by the U.S. Department of Defense (DoD) for critical military operations, risks due to technical failures in the control segment are judged to be relatively minor compared to other risks. Potential problems include software or hardware updates to the control segment, which could have unintended consequences.

The DoD ensures a high level of reliability by implementing a control segment design featuring a high level of redundancy. For example, every GPS satellite can be seen from at least two monitor stations at all times. Also, the Jet Propulsion Laboratory (JPL) operates a global network of GPS receivers that measure the reliability of the GPS civilian signals. If a problem occurs, an alarm can be triggered and sent to multiple operations centers within 4 seconds, in order to alert users that the integrity of the GPS signal may be compromised.

Despite these measures, problems can and do occur. For example, in January 2010 the GPS Wing of the U.S. Air Force implemented a software grade which caused a small number of military GPS receivers to experience loss of GPS lock or the inability to acquire satellite signals altogether. This problem, however, was limited only to some military users using a specific subset of receivers.

This episode, however, highlights the potential for future upgrades to affect even civilian users. It is expected that this risk is mitigated by a comprehensive testing program before any widespread software upgrade is initiated. Such risks, however, cannot be reduced entirely to zero.

III.II Space segment

Unintended interference

Unintended interference can be caused by other radio transmitters that are working nearby the frequencies used by the positioning satellites (L1=1547,42 MHz , L2=1227,60 MHz)[24]. Weakly shielded or faulty electronics can cause interference, too.

Intentional interference

Intentional interference can be caused by sending interfering signals on the same frequency band that the satellite systems are using. Equipment that is used to generate interfering signals is called a jammer. GPS-jammers are quite easily available via the Internet, and they are inexpensive[24]. Prices for portable devices are starting from around $30, and the effective range is 2-300m.

Atmospheric conditions

The ionosphere and troposphere can cause variation of the speed of the GPS signal. Speed variation can cause 0-30m errors[26].

Multipath propagation

Multipath propagation occurs when the signal is reflected from surrounding elements like buildings. Multipath propagation can cause 1 meter error[26].

Selective availability

For the GPS system the U.S. Department of Defence can make intentional alteration of the time and epherimis signal, called Selective Availability (SA). SA can cause 0-70m errors[26]. SA for civilian service was stopped on May 2000, but it is still technically possible for U.S. to execute.

Total signal loss

Total signal loss can occur when contact with the satellites is lost. These situations can occur in tunnels or parking garages.

III.III User segment

The tracking device is complicated construction and it combines the functionalities of the GPS receiver and mobile phone. Many times, depending on application, it has to work in the demanding environment and it is vulnerable for many environmental threats. Following chapters describes the main threats.

HW fault

Hardware faults can occur due to environmental variables or other causes. Typical causes are mechanical stress, temperature change, high humidity, and aging.

SW fault

Software faults can occur in the operating system or in applications. SW errors can cause processing errors, data output errors or processing delays.

Power feed breakdown

The power feed for a tracking device can be external power source or internal batteries. Power feed breakdown can halt use of the tracking device completely.

Clock drift

The internal clock of the GPS receiver is not precise compared to atomic clocks onboard the satellites. Clock drift can cause 0-1.5m error[26].

Signal attenuation / Measurement noise

Signal attenuation can occur if the tracking device is installed improperly or there are mechanical faults in antenna lines. Signal attenuation can cause 0-10m error[25].

Information security

It is theoretically possible to hijack a smart phone and steal data. As more and more different smart phones come to the market including different software and applications, information security is in a key role in the future. These threats already exist. Vulnerabilities have already been found for the iPhone[27] and Android[28]. This is a potential risk in the near future.

III.IV Communication segment

The usage of the internet has increased communication network load rapidly and application guaranteed service quality can be offered very rarely. The security issues are many times in secondary role or they are even ignored. It is important to know the technical risks of the communications networks because it speeds up problem solving and test case analyzing. Following chapters presents the basic technical risk of the communications networks.

Mobile phone intentional interference

Intentional interference can be caused by sending interfering signals on the same frequency band than radio network is using. Equipment that is used to

generate interfering signals is called a jammer. Mobile phone jammers are quite easily available via the internet, and they are inexpensive[29]. Multifunctional devices can generate interference for radio network frequencies and GPS. Prices for portable devices start at around $30, and the effective range is 2-20m.

Mobility

When the mobile phone is moving in the network it performs actions like cell hand overs, inter system handovers, location area updates and routing area updates. In some cases the mobility can cause additional delay or even data loss if the data connection is cut off during mobility action. Environmental variables can cause changes for the quality of the radio signal.

GPRS/3G capacity

GPRS user plane capacity could be a problem in highly populated areas. Rapidly growing use of mobile internet causes stress for mobile networks. Rural areas could have very limited GPRS capacity, or there may not be GPRS capacity at all. High amount of mobility requires network signalling capacity. There have already been cases reported of capacity problems[32].

GPRS/3G latency

Round-trip time (RTT) in GPRS can vary a lot, and it can be greater than 1000ms. 3G offers much lower RTT compared to GSM. RTT is typically 200-300 ms.

GPRS/3G information security

GPRS and 3G offers data encryption only on the radio interface. Data is delivered without encryption in the core network[30].

GPRS/3G radio coverage

Although GSM offers connectivity in more than 218 countries and covers more that 80% of the world's population[11], there are still areas that are not covered by GSM[12], including parts of Canada, South America, Africa, Russia and Australia. Europe is well covered with GSM.

3G has good radio coverage in North, West and South Europe. Other parts of the world are expanding their networks[12].

GPRS/3G roaming

Roaming is the situation when a device is moving outside of home network[31]. Roaming can cause situation when the mobile is not able to deliver location data via packet switched services.

Internet capacity

Capacity depends on used access network capacity, core network capacity and current network load.

Internet latency

Delivery time of the data depends on the capacity of the access network being used, as well as the current network load and distance between delivery points.

Internet information security

Data is not encrypted as default when delivered via Internet. Unsecured and sensitive data can be potential target for the hackers.

III.V Data processing segment

The location data is stored and processed by servers that offers user interface too. For the end user is essential that service cluster offers secure and reliable service. Following chapters describes the main vulnerabilities of the service cluster.

HW fault

Hardware faults can occur by environmental variables. Typical variables are mechanical stress, temperature changes, great humidity and aging.

SW fault

SW fault can occur in operating system or in application. SW error can cause processing errors, data output errors or processing delays.

Power feed breakdown

Power source failure can cause partial or total service outage.

Processing capacity

The large number of the transactions in some applications requires significant processing capacity. Lack of capacity can cause system malfunction.

Information security

Location data is delivered and accessed via external networks. The data center where the information is stored has to be protected properly against external security threats (virus, DOS-attack, etc).

Database corruption

Database corruption can cause loss of history data. Database corruption can be caused by e.g. hard disk failure or electricity break.

III.VI End user segment

The location information can be accessed with a computer or mobile client, depending on the application. Typically the user interface is offered via internet connection and web browser. Possible vulnerabilities are weak password, weak virus protection and unshielded internet connection.

The latest versions of the smart phones like iPhone and Android based mobiles are more and more like computers than legacy mobiles. This evolution has caused that they have became vulnerable for the same threats than computers.

IV. FIELD TEST SETUP DESCRIPTION

For field testing we had to build up testing environment. We used a smart phone as a tracking device in parallel with real GPS receiver. We executed all the tests in Finland and we used Finnish mobile network service providers.

Tracking data was logged both in the smart phone, in the GPS receiver and in the server. After test logs were downloaded for post processing.

Used field test setup is described in Figure 2.

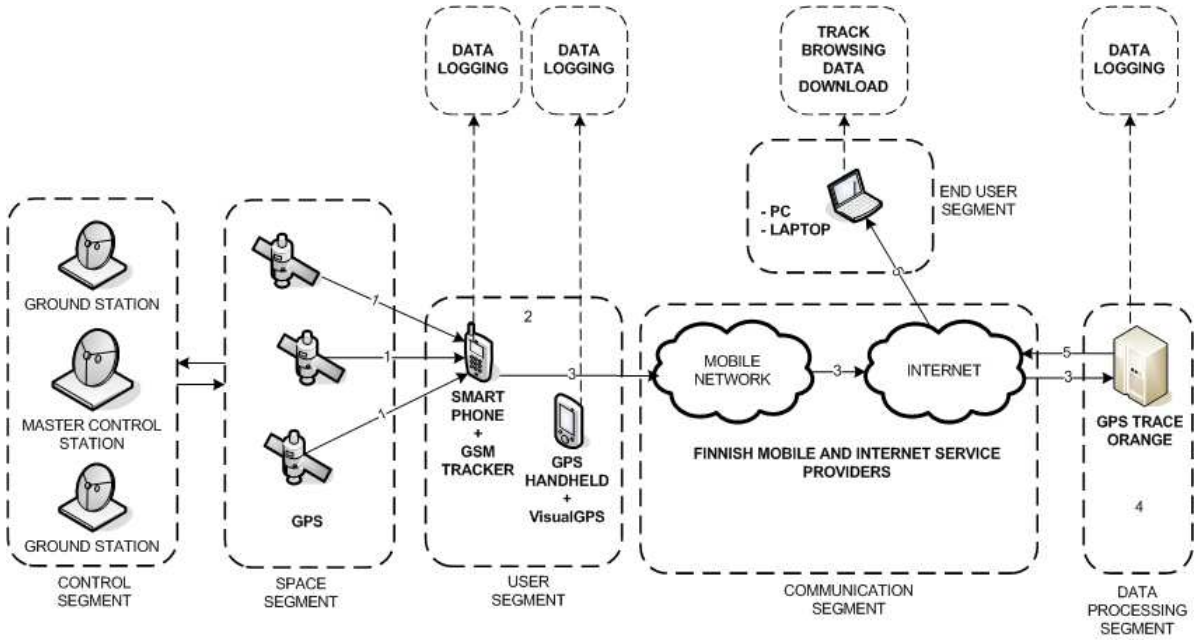


Fig. 2: Field test setup.

IV.I Control segment and Space segment

We used smart phones in this test because most of the smart phones nowadays support GPS navigation and tracking. GPS tracing equipment are commonly available and they are cheap. Other positioning and tracking systems than GPS were not available for this research.

IV.II User segment

Smart phone

Nokia smart phone N95[33] (V31.0.017) was used as tracking device. Nokia N95 is equipped with the TI GPS5300 GPS chip that supports Assisted GPS (A-GPS)[34]. The smart phone was equipped with the GSM Tracker 3 (v3.22)[35] application. GSM Tracker uses the GPS of the smart phone and forwards location data in NMEA[36] format via wireless networks to the selected tracking service. Used smart phone is presented in Figure 3.

Fig. 3: Nokia N95 smart phone

The GSM Tracker offers many options to set location triggers and logging options. The user can define time and distance triggers for location triggering. GSM Tracker is able to save location data

to the file in NMEA format in parallel with mobile network information (cell id). Logs from the mobile were transferred for the post processing via USB connection. The screen shot of GSM Tracker is presented in Figure 4.

Fig. 4: GSM tracker screen shot

GPS receiver

GPS receiver PhotoNav[37] was used in parallel with Nokia N95. Photonav is equipped with SiRF Star III GPS chip and WindowsCE 5.0 operating system.

VisualGPSce[38] was used for real time signal browsing and as logging application. Location data was stored in NMEA format. Photonav supports high capacity secure digital memory cards. Photonav with VisualGPSce is presented in Figure 5.

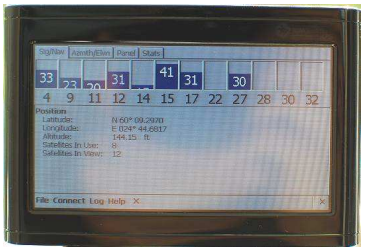


Fig. 5: Photonav GPS receiver with VisualGPSce

IV.III Communication segment

We used services of the Finnish mobile network operators (Elisa and Sonera). Elisa and Sonera offer modern mobile network services that support GPRS, EDGE, 3G and HSDPA data services. The largest cities are covered with 3G and more rural areas with 2G. Both operators offer very good network coverage in Finland.

IV.IV Data processing segment

GPS Trace Orange[39] offers web based free service for satellite based tracking. The service supports about 100 different tracking devices. The user can follow tracked device in real time or the racking data can be downloaded in four forms (OziExplorer, NMEA, Google Earth, Wialon). The location data is stored for 30 days and then it is deleted automatically.

The tracking device is recognised by IMEI number and the location data is received in NMEA format. The screen shot of the GPS Trace Orange is presented in Figure 6.

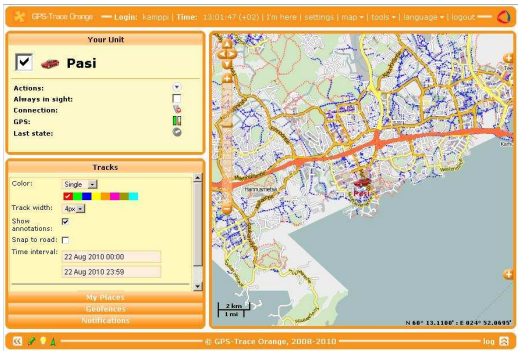


Fig. 6: GPS Trace Orange screen shot

IV.V End user segment

PC and laptop was equipped with Windows XP operating system. Microsoft Internet Explorer or Mozilla Firefox was used as web browser.

V. TEST CASES

V.I Stationary tracking

Accuracy tests were executed by stationary tracking. The smart phone and GPS receiver was located in the car during one hour. Tracking devices were covered with sun shields, Figure 7.

Fig. 7: Smart phone installed in the car

The car was parked on the roof top of the parking garage or on the ground level parking place. The reference location was estimated with the map service (Kansalaisen Karttapaikka)[40].

After testing logs were downloaded from the GPS devices for the post processing

V.II Rural and long haul tracking by car

The purpose of the rural and long haul testing was to find out reliability of the location data transfer via mobile networks. Routes contained roads (max 100 km/h) and high ways (max 120 km/h). Test duration was several hours per track and. length up to 350 km.

Testing route was covered with GPRS, EDGE and 3G mobile networks. Cell changes and inter system handovers were logged too. The smart phone was located on the top of the console. GPS receiver was not used in test case. Figure 8 present how the smart phone was installed in the car.

Fig. 8: Smart phone installed in the car

V.III Urban tracking by car

The main purpose of this test case was to find out how urban environment (buildings, urban canyons, tunnels) affects to GPS tracing accuracy. Test was executed with the car in the Helsinki capital area. Figure 9 presents how the GPS devices were installed in the car.

Fig. 9: Nokia N95 and Photonav GPS receiver installed in the car

V.IV Open water tracking

Tracking on the open water was executed with the boat on Saimaa lake district in Finland. The duration of the test was several hours. The speed of the boat was constant 18 km/h. The smart phone was installed like in figure 10.

Fig. 10: Smart phone in the boat

V.V Bicycling

The smart phone was located on the top of the back bag or in the side pocket of the bicycling shorts during bicycling exercise, figure 11.

Fig. 11: Smart phone with bicycling equipment

Test duration was 30-120 min and the length of the trip up to 40 km per exercise. The purpose of this test case was to find out how smart phone performs with fitness activity.

VI. RESULTS

Below we present the results from the results from our various measurements using the test set-up described above. This section is divided into subsections based on the type of measurement being

performed, including position precision and data loss rate.

VI.II Position Precision of Fixed Locations

In order to obtain a baseline measurement, we decided to conduct a "stationary" tracking test, where the tracking device was kept stationary in an open area for about one hour periods at different times of the day on three consecutive days. Two different locations were used, but they are relatively nearby each other and exhibit similar sky visibility characteristics. From the resulting data logs, we calculated the mean longitude and latitude measured by the device and the standard deviation for these measurements. The standard deviation was then converted to an approximate distance in meters using the following equations:

$$d_{lat} = \alpha_{lat} \times (1.114 \times 10^5 \frac{m}{degree})$$

$$d_{long} = \alpha_{long} \times (5.580 \times 10^4 \frac{m}{degree})$$

where d_{lat} is the distance in the north-south direction in meters, α_{lat} is the standard deviation in latitude in degrees, 1.114×10^5 is the number of meters in one degree latitude at 60º latitude, d_{long} is the distance in the east-west direction in meters, α_{long} is the standard deviation in longitude in degrees, and 5.580×10^5 is the number of meters in one degree longitude at 60º latitude. Since all of our measurements occur at approximately 60º latitude, this approximation should be sufficient for this level of analysis.

We also record for each test case the average number of satellites detected and the average Horizontal Dilution of Precision (HDOP), which is a measure of expected precision based on the configuration of the GPS satellites used in the position calculation. We repeated these measurements using both the PhotoNav GPS receiver and the N95 mobile device. The results are presented below in tables 1 and 2 below, respectively.

GPS Receiver

Day	Time of Day	Duration	# of Fixes	Mean # of Sats.	Mean HDOP	Mean Long. (degrees)	σ Long. (m)	Mean Lat. (degrees)	σ Lat. (m)
Day 1	Morning	1:06:26	3987	10.8	0.829	60.22526	1.829	24.75572	1.350
Day 1	Evening	1:04:49	3890	7.0	1.546	60.15515	4.450	24.74468	4.697
Day 2	Morning	0:40:49	2450	10.1	0.928	60.22518	0.535	24.75581	1.571
Day 2	Evening	1:00:36	3637	7.4	1.401	60.15525	0.265	24.74478	0.637
Day 3	Morning	1:30:02	5403	10.4	0.874	60.15523	0.156	24.74489	0.809
		Total	**19367**			**Average**	**1.4313**	**Average**	**1.7654**

Table 1:Measurements with GPS Receiver

Mobile

Day	Time of Day	Duration	# of Fixes	Mean # of Sats.	Mean HDOP	Mean Long. (degrees)	σ Long. (m)	Mean Lat. (degrees)	σ Lat. (m)
Day 1	Afternoon	0:49:57	497	6.0	1.767	60.15524	1.768	24.74471	0.763
Day 1	Evening	0:56:27	563	6.4	1.849	60.15524	2.016	24.74473	1.117
Day 2	Morning	0:40:05	399	6.9	1.537	60.22528	4.586	24.75570	1.891
Day 3	Morning	1:28:55	884	7.1	1.285	60.15524	1.022	24.74470	0.709
		Total	**2970**			**Average**	**2,0260**	**Average**	**1,0198**

Table 2: Measurements with Mobile phone

Day	Time of Day	Duration	# of Fixes	Mean # of Sats.	Mean HDOP	Mean Long. (degrees)	σ Long. (m)	Mean Lat. (degrees)	σ Lat. (m)
Day 3 High	Morning	1:28:55	884	7.1	1.285	60.15524	1.022	24.74470	0.709
Day 3 Low	Morning	1:02:17	627	4.7	2.495	60.15521	8.122	24.74469	3.800
		Total	**2970**			**Average**	**3,9681**	**Average**	**1,9916**

Table 3: Difference between High sensitivity and Low sensitivity modes

By comparing these tables, we can see that the GPS receiver generally gives a higher level of precision due to its ability to detect a higher number of satellites (on average). There is, however, a significant variability in the number of satellites detected for each test run, which in turn affects the

HDOP and standard deviation of the position measurements. This is mostly due to the fact that the satellites are constantly moving in their orbits, so during different segments of the day, there are a different number of satellites in the field of view of the GPS receiver. This can also be seen in Figure 12 below, which shows a histogram of the number of satellites detected for the GPS receiver and mobile device, respectively.

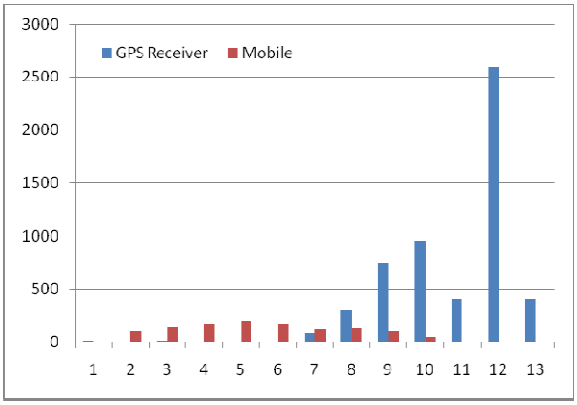


Fig 12:Histogram of the number of satellites detected

During our measurements, we noticed that the sensitivity of the mobile device is affected by the position of the slide-out keyboard. This is due to the fact that the GPS module is installed directly below the keyboard, so if the keboard is positioned in the "out" configuration, the sensitivity is much higher. We therefore call this configuration "high sensitivty mode," whereas the closed position we call "low sensitivity mode. This difference can be clearly seen in Table 3, where we present two different measurements in high and low sensitivity mode, respectively. Similarly Figure 13 below shows the difference in HDOP value between high sensitivity and low sensitivity mode.

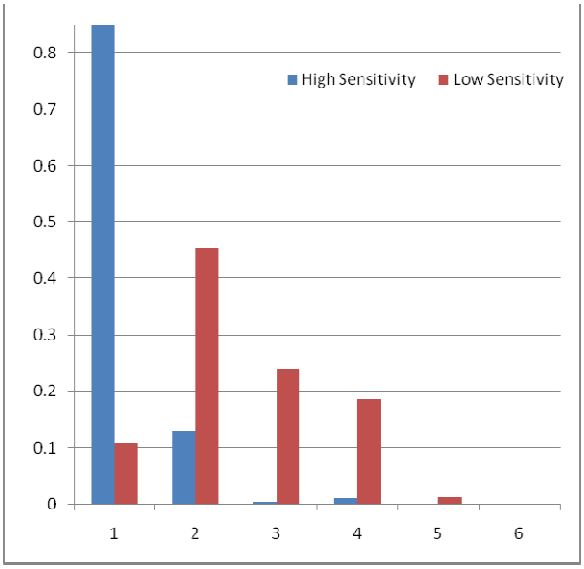


Fig 13: Difference in HDOP value between high sensitivity and low sensitivity mode

Figure 14 below shows these precision measurements distributed on a geographic plot. We can see the position measurements from the mobile device are distributed over a wide area, but mainly concentrated in a 4 m radius circle. When the mobile device was in "low sensitivity mode", the positions are much less concentrated around one area (i.e. higher standard deviation). For the GPS receiver, the position measurements are quite concentrated in one area, however, we noticed during these measurements was the position gradually and consistently moved from east to west. We surmise that there is perhaps some software error or averaging function in the device which causes this undesirable behavior.

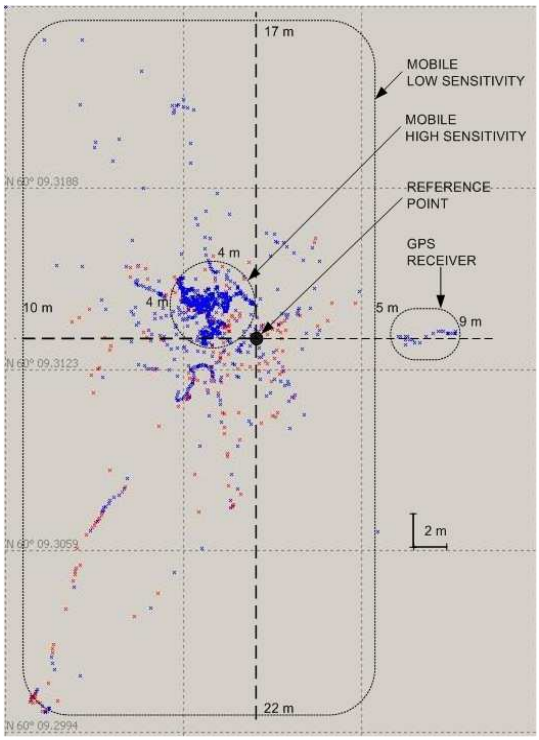


Fig. 14: Stationary test, horizontal plot

Figure 15 shows a plot of the vertical component of the position measurements for our stationary tests. Here you can clearly the difference in precision between the GPS receiver and the mobile device in both low sensitivity and high sensitivity mode.

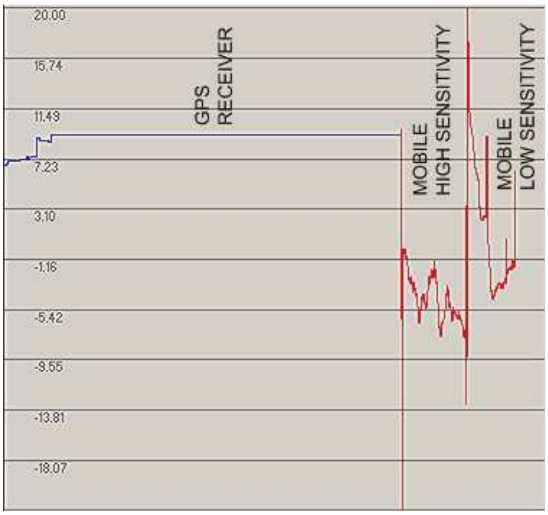


Fig. 15: Stationary test, vertical plot

VI.III Data Loss Rate

In order to measure the rate of GPS data loss, we conducted various mobile tracking measurements for different use cases, described in Section V above. Afterwards, we compared the mobile logs with the logs stored on our third-party server to determine how many measurements were successfully sent to the server. The results are shown below in Table 4.

Data loss can occur due to a variety of factors. In our tests, buffering was activated in the mobile device, so if there was no mobile network, the position measurements could be sent once network coverage resumed. There is a limit, however, to the size of the buffer, and in the rural driving case, we reached this limit. Another source of data loss is the inability of the device to generate an "active" GPS fix, due to obstruction or other factors. The software is designed to record a time measurement in the mobile log, but not to send this measurement to the server. So this is a second source of data loss, due to the unavailability of the data itself.

We can see from this table, however, that the rate of data loss is quite low for the use cases under investigation. It was highest for the suburban bicycling case, probably due to the fact that the device was obstructed by the user's backpack, body, and/or clothing.

Day	Total # of Fixes	# of Active Fixes	Number Received by Both	Number Recorded by Mobile Log	Number recorded only by Server	Percentage of Total	Percentage of Active
Rural car driving	**17719**	**17456**	**17438**	**279**	**2**	**98.4%**	**99.9%**
Suburban driving	**2784**	**2661**	**2661**	**123**	**0**	**95.6%**	**100%**
Urban Driving	**1175**	**1163**	**1162**	**13**	**0**	**98.8%**	**99.9%**
Suburban Bicycling	**3064**	**2771**	**2770**	**274**	**0**	**90.4%**	**99.9%**
Sailing in Gulf	**970**	**969**	**969**	**1**	**0**	**99.9%**	**100%**

Table 4: Comparison of the mobile logs with the logs stored on our third-party server

VII. DISCUSSION

VII.I General observations

GSM Tracker is easy to use and offers versatile options for the settings. In everyday use the GSM Tracker was very reliable and worked very smoothly.

GPS Trace Orange is easy to use and offers basic service for satellite based tracking. The service could have better security because it supports only http protocol. GPS Trace Orange is very reliable GPS tracking service.

Mobile network service and coverage in Finland is quite good. Operators are upgrading their networks constantly and the latest features are supported.

VII.II Rural and long haul tracking by car

Smart phone battery consumption is high when the GPS is activated. We didn't make any measurements for the battery consumption but the battery had to be charged more often than without GPS. Usage of the continuous power feed is recommended if it is possible. In the summer the smart phone heats up in the sun shine if the smart phone is placed on the top of the console.

Once mobile logging buffer filled up and tracking was stopped. The reason was that there were many previous logs on the flash drive of the mobile. Only once mobile Internet connection was lost and the tracking application was restarted manually.

VII.III Urban tracking by car

The results of the stationary tracking shows that the sensitivity of the smart phone with GPS is lower compared to the GPS receiver. For that reason we didn't make any calculations for the urban trace logs but we uploaded the NMEA data to the Google Earth for the visual inspection. Plotted routes didn't differ remarkably from the each other and the performance of the smart phone was quite satisfactory.

VI.IV Sailing

Map offered by the GPS Trace orange is not suitable for the tracking boats. The map of the tracking service does not offer detailed information about lake or sea areas. The tracking data needs to be downloaded from the service and could be combined with the navigational chart.

VII.V Bicycling

The smart phone is not suitable for the serious fitness usage. The smart phone does not stand moisture or hard mechanical stress. The durability of the battery could limit the usability in the long term exercise. The mobile could be covered with the shield for extra protection.

VII.VI Incoming circuit switched call

While using the smart phone as a tracking device we have to remember that it is still a mobile phone too. Incoming circuit switched call can cause interruption for the active GPRS session and the GPRS connection is suspended during circuit switched call. This feature can cause interruption for the real time location tracking. If the tracking device supports buffering the tracking data is delivered to the tracking service when GPRS connection is released from the suspension. 3G supports simultaneous packet data and circuit switched connections.

We faced this situation a few times without data loss because our tracking device supports buffering.

VII.VII DOS attack

When a smart phone has an active packet data connection it has an IP-address. The host with the IP-address is vulnerable for the security attacks if the network and the host are not protected properly.

We noticed that it is possible to interfere a single smart phone user by sending data to the user without user request. We sent dummy UDP-data to the mobile host from the fixed line by using iperf application. The network was not protected properly and our data load was routed to the mobile. The capacity was reserved from the radio interface and the internet

connection of the mobile became unusable. In practise it is possible to scan mobile network with one mobile host and make DOS attack against all active users.

DOS attack could cause interruption for the real time tracking or the battery of the mobile phone will drain very fast.

VIII. CONCLUSION

Satellite based tracking systems are widely used in real life but there is very rarely described how the system can be tested. The system is complicated and building of field testing environment requires a lot of knowledge and expertise. The Laurea University of Applied Sciences has built up competence in the area with Saterisk project and it made this research possible.

We found that basic functionality is very reliable and the system level performance is quite good. Especially modern telecommunication network can offer reliable data transfer path for the satellite based tracking application. We found that data transfer reliability is 99.9 percent when tracking device supports buffering in case that there are connectivity problems. However, the test set was executed only in Finland and more testing is needed in international environment.

Modern smart phone includes integrated GPS and navigation functionality. Our tests revealed that the smart phone with much functionality is a compromise. The GPS sensitivity is worse to compared real GPS receiver. The smart phone was able to detect 2 to 10 satellites when the GPS receiver detected 7 to 13 satellites in the same environment. The measured mean stationary longitude deviation was 2,03m and mean stationary latitude deviation was 1,02m. This observation doesn't directly reflect to accuracy as expected and more testing is needed.

We also noticed that the mechanical design of the smart phone can have affect to the GPS performance. The used smart phone (Nokia N95) has slide-out keyboard and the GPS sensitivity is remarkable higher when the keyboard is exposed. The reason is that the GPS chip is located under the keyboard.

A smart phone can offer satisfactory consumer level user experience with satellite based tracking service but in professional use it is more reasonable to consider other options. Dedicated tracking devices can offer more mechanical durability and they are not vulnerable for security risks like smart phones.

Laurea University of Applied Sciences will continue field testing with satellite based tracking systems. The next phase is to create database for tracking data and automate tracking data analysis.

[1] Inside GNSS, About GPS, http://www.insidegnss.com/aboutgps

[2] U.S Air Force, Airmen upgrade GPS constellation, http://www.af.mil/news/story.asp?id=123207262

[3] Inside GNSS, About GLONASS, http://www.insidegnss.com/aboutglonass

[4] Russian Federal Space Agency, Information-Analytical Centre, http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:20:1122524503041832::NO

[5] Inside GNSS, About Galileo, http://www.insidegnss.com/aboutgalileo

[6] Inside GNSS, About Compass, http://www.insidegnss.com/aboutcompass

[7] National Aeronautics and Space Administration, Spacewarn Bulletin, August 1st 2010, http://nssdc.gsfc.nasa.gov/spacewarn/spx681.html

[8] Aspicore, GSM Tracker application, http://www.aspicore.com/en/tuotteet_tracker.asp

[9] Motorola, MTM800E TETRA mobile, http://www.motorola.com/Business/XU-EN/Product+Lines/Dimetra+TETRA/TETRA+Terminals/TETRA+Mobile+Radios/MTM800_Enhanced_XU-EN_PK-EN_XF-EN_XN-EN_XC-EN_XM-EN_XE-EN

[10] 3GPP, GPRS, http://www.3gpp.org/article/gprs-edge

[11] GSM World, GSM, http://www.gsmworld.com/technology/gsm/index.htm

[12] GSM World, 2009, GSM WorldPoster2009a, http://www.gsmworld.com/roaming/GSM_WorldPoster2009A.pdf

[13] 3GPP, UMTS, http://www.3gpp.org/article/umts

[14] 3GPP, HSPA, http://www.3gpp.org/HSPA

[15] 3GPP Technical realization of the Short Message Service (SMS), 3GPP TS 23.040 v8.6.0

[16] 3GPP, LTE, http://www.3gpp.org/LTE

[17] TETRA MoU Association, http://www.tetramou.com/tetramou.aspx?id=44

[18] TETRA MoU Associaton, TETRA Release 2, http://www.tetramou.com/tetramou.aspx?&id=1186

[19] WiMAX.com, What is WiMAX, http://www.wimax.com/education

[20] WiMAX FORUM, 2010, Monthly Industry Report, http://www.wimaxforum.org/resources/monthly-industry-report

[21] PCMag.com, Definition of API http://www.pcmag.com/encyclopedia_term/0,2542,t=API&i=37856,00.asp

[22] GpsGate.com, API http://gpsgate.com/go/gpsgate/dev_guide.asp

[23] Kämppi, Pasi, Robert Guinness, 2010, Technical Risk Analysis for Satellite Based Tracking Systems, Integrated Communications Navigation and Surveillance Conference (ICNS), Herndon

[24] InsideGNSS, About GPS,
http://www.insidegnss.com/aboutgps

[25] Jammer World, GPS Jammer,
http://www.thejammerworld.com/product_GPS_Jammer_GPS_Jammer_page_1.html

[26] Cmtinc.com, Gpsbook, Chapter Six: The GPS Error Budget,
http://www.cmtinc.com/gpsbook/index.htm

[27] Mogull Rich, 2009, The iPhone's SMS Vulnerability, MacWorld
http://www.macworld.com/article/142179/2009/08/iphone_sms_security.html

[28] Sadun Erica, 2009, Android security vulnerability discovered, Ars Technica
http://arstechnica.com/open-source/news/2009/02/android-security-vulnerability-discovered.ars

[29] Jammer World, Mobile Phone Jammer,
http://www.thejammerworld.com/product_Mobile_Phone_Jammer__page_1.html

[30] Kämppi, Pasi, Jyri Rajamäki, Robert Guinness, 2009, Information security in satellite tracking systems, 3rd International Conference on Communication and Information Technology, Athens, pp. 153-157

[31] GSM World, Mobile SMS and Data Roaming Explained,
http://www.gsmworld.com/documents/sms_data_roaming_explained.pdf

[32] Sarno David, Los Angeles Times, 2009, http://articles.latimes.com/2009/dec/10/business/la-fi-iphone10-2009dec10

[33] Nokia N95 description, http://www.nokia.co.uk/support/product-support/nokia-n95

[34] Nokia A-GPS, http://europe.nokia.com/support/product-support/nokia-n95/a-gps

[35] GSM Tracker, http://www.aspicore.com/en/tuotteet_tracker.asp?tab=2&sub=1

[36] NMEA data description, http://www.gpsinformation.org/dale/nmea.htm

[37] Photonav GPS receiver description, http://www.verkkokauppa.com/popups/prodinfo.php?id=11150

[38] VisuaGPSce, http://www.visualgps.net/VisualGPSce/default.htm

[39] GPS Trace Orange, http://gps-trace.com/

[40] Map service, Kansalaisen Karttapaikka,
http://kansalaisen.karttapaikka.fi/kartanhaku/osoitehaku.html?e=406643&n=7195132&scale=8000000&width=600&height=600&tool=siirra&lang=en