jamk.fi

Implementing security controls in existing system

Henri Savonen

Master's thesis
December 2016
Technology, communication and transport
Master's Degree Programme in Information Technology

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Savonen, Henri	Type of publication Master's thesis	Date December 2016
		Language of publication: English
	Number of pages 45	Permission for web publication: x

Title of publication
Implementing security controls in existing system

Degree programme
Masters's Degree Programme in Information Technology

Supervisor(s)
Häkkinen, Antti; Karjalainen, Mika

Assigned by
Patria Aviation Oy

Abstract

The main objective is the investigation of possibilities of elevating existing and old information system to comply with the current information security criteria. The elevation process of one system security is included, in which one system already in production will be made to fulfill the requirements of current national auditing criteria.

The subject is topical in the field of cyber security, as according to the national criteria, problems in information security are to be noticed in the planning phase; however, this has proven to be impossible in practice. The current cyber threats and best practice models (VAHTI, ISO207001, KATAKRI, etc.) are used as the theoretical framework.

The study was conducted as a qualitative case study divided into three cases. The aim was to find the threats, how to mitigate them and also find the differences between commonly presented practice models and auditing criteria when dealing with an existing and a new system.

If the anti-malware software cannot be installed in the target environment, it is not possible to detect security issues taking place when imported data is extracted and used in the environment. If the system is not updateable, then the continuous development and OODA loop will also be easily broken. One broken part of the OODA loop affects the functioning of all other parts.   If the system is newly procured, it is easier to keep track of all publicly available information and make contracts limiting all the information usage and publication.

In the light of this thesis, it seems to be impossible to measure how the system hardening was carried out if defensive and detection mechanisms are not tested and trained.

Keywords/tags (subjects)

KATAKRI, Information Security, Comprehensive security

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t) Savonen, Henri	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Joulukuu 2016
		Julkaisun kieli Englanti
	Sivumäärä 45	Verkkojulkaisulupa myönnetty: x

Työn nimi

Implementing security controls in existing system

Tutkinto-ohjelma

Mastes’s Degree Programme in Information technology

Työn ohjaajat(t)

Häkkinen, Antti; Karjalainen, Mika

Toimeksiantaja(t)

Patria Aviation Oy

Tiivistelmä

Opinnäytetyön päätavoite oli tutkia jo olemassa olevan ja vanhan tietojärjestelmän mahdollisuuksia vastata tämänhetkisiin tietoturvakriteereihin. Työn käytännön osuuden aikana tehtiin yhden järjestelmän turvallisuuden korottaminen, jossa jo tuotannossa olevaa järjestelmää muokattiin siten, että se vastaisi tämänhetkisen kansallisen auditointikriteetistön vaatimuksia.

Aihe on ajankohtainen kyberturvallisuuden alalla, sillä kansallisen auditointikriteeristön mukaan tietoturvan ongelmat tulisi ottaa huomioon jo suunnitteluvaiheessa, mutta se on osoittautunut käytännössä mahdottomaksi. Teoreettisena viitekehyksenä on käytetty tämänhetkisiä kyber-uhkia ja parhaita toimintamalleja (VAHTI, ISO207001, KATAKRI, jne.).

Tutkimus on toteutettu laadullisena tapaustutkimuksena ja jaettu kolmeen caseen. Tavoite oli löytää uhkia, kuinka rajoittaa niiden vaikutusten haitallisuutta, sekä löytää eroja yleisesti esitettyjen parhaiden toimintamallien ja auditointikriteerien välillä, kun käsitellään vanhaa ja uutta järjestelmää.

Jos tietoturvaohjelmistoa ei voida asentaa kohdeympäristöön, ei tapahtuvia turvallisuusseikkoja voida havaita, kun ulkopuolelta tuotua dataa puretaan käyttöön ympäristössä. Jos järjestelmä ei ole päivittyvä, jatkuva kehitys häiriintyy ja OODA-silmukka rikkoutuu herkästi. Jos silmukan yksi osa rikkoutuu, se vaikuttaa myös kaikkien muiden osien toimintaan. Jos järjestelmä on uusi, on helpompi pysyä selvillä kaikesta julkisesti saatavilla olevasta tiedosta sekä tehdä sopimuksia, jotka rajoittavat tiedon käyttöä ja julkaisua.

Tulosten valossa vaikuttaisi olevan mahdotonta mitata, miten järjestelmän koventaminen on tehty, jos tunnistus- ja torjuntamenetelmiä ei testata ja niiden käyttöä ei harjoitella.

Avainsanat (asiasanat)

KATAKRI, Tietoturva, Kokonaisturvallisuus

Muut tiedot

Contents

Figures

Acronyms and Abbreviations

AMT	Intel Active Management Technology
APT	Advanced persistent threat
ATA	AT Attached, old connection name for hard disk
CGM	Cots, Governmental and Military Software
CIA	Confidentiality, Integrity and Availability
COTS	Commercial off-the-shelf
DMA	Direct Memory Access
HID	Human Interface Device
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
ILO	Hp Integrated Lights-Out technology
KATAKRI	National Security Auditing Criteria
NH90	NHIndustries NH90 (NATO Helicopter 90)
OODA	Observation Orientation, Decision making and Acting
PLC	Power Line Communications
RDP	Remote Desktop Protocol
SATA	Serial AT Attachment
TPM	Trusted Platform Module
USB	Universal Serial Bus

1 Introduction

The motivation behind this study the ongoing work with existing systems and the implementation of information security measures onto pre-existing systems. The commonly accepted preferable approach to system security is to implement security measures at the time of the procurement of the system as a whole. This study concentrates on comparing the differences between the implementation processes and the auditing of implementation processes of security systems implemented on both existing and pre-existing systems.

Cyber security and information security business are currently trending industries. The auditing and building of secure systems is a growing business in the context of contemporary information technology and business world. Current Finnish Law requires for public contracts to implement certain information security requirements to be set for any new systems procured or to be procured by public entities. This is dependent on the intended use of the system and the area of government operating the system. (A 1.7.2010/681)

Many of the currently used systems have been implemented before the publication of the current auditing criteria, laws and guidelines. In addition, many of the systems currently in the implementation phase have been procured before the publication of the auditing criteria, laws and guidelines. These systems do, however and somehow, have to be implemented and made to comply with the current auditing criteria, laws and guidelines. Compromises are, however, required as all of the current standards cannot be met by many of these systems and forcing these systems to comply with all these standards can be counterproductive.

2 Research goals

The aim of the study was to explore the differences between the new system, where the security requirements are considered already in contract phase, and the hardening of the old system.

The aim was to create a model that can be used to bring information security controls into the existing system, as qualitatively and precisely as possible. The main focus is on differences between implementing the new system and hardening the existing or previously purchased system. The research of the topic is necessary in order to gain the knowledge, how to identify the balance between the threats, assets that need to be protected, and information security controls.

It is neither possible nor appropriate to fulfill all current standards. The system itself may include properties that are against current information security requirements. In addition, the current requirement and legislation did not exist when the existing system was engineered. Therefore, it may not be necessary to fulfill all the current requirements.

Information Society code 971/2014, Ohje tietoturvallisuuden arvitointilaitoksille 210/2016 O and KATAKRI National Security Auditing Criteria 2015 have been updated all between 2014 and 2016. Therefore, their requirements were not involved in procurement of information security system. In military industry purchasing processes may last even up to ten years, and the life cycle of the systems may be measured in decades. Therefore, legislation, threats and technology develop much faster than the applications. (Tietoturvakaari, Information Society code 971/2014.)

National security auditing criteria describe for example some requirements for contract with organization or company. The personnel of a company should have a certain required level of security awareness. During software development some security controls, like static code analysis, should be implemented in order to avoid unsafe functions in code etc. (KATAKRI 2015 I 13.)

Security auditing of an existing system, that has been in use previously, is outside of the scope of this thesis. An existing system in this case means that system is installed securely on new hardware and the risks are minimized by that kind of counter measures. Security vulnerabilities of an old information system referred to in this thesis are risks that are caused by other means. Lack of system updates or publicly known vulnerabilities are for example huge known risks. This might be caused by fact that a software supplier does not accept some updates, or updates are not tested and approved by a supplier.

Other risks of this kind are caused by the fact that software might also be in use by other users, and default passwords, configuration files, source code or user manuals might be publicly available at the time. It is not necessarily written in to the original contract that supplier should not sell the same software and documentation for other users and countries. This might expose vulnerabilities for hostile actors.

One goal in this study is to identify possible security issues that cannot be fixed neither by hardening nor adding additional security measures. Threats that are identified should also be taken under consideration. Risks should be mitigated as far as it is possible, however, even after that there still remain completely unknown vulnerabilities. Even though there will always remain that black swan and unknown risk, it should not be cause for an uncontrolled situation. This remaining unknown part is outside the scope of this work and is more a part of the continuity management process.

3 Research method

The method of the study is a case-study, focusing on auditing criteria and and fulfillment of minimum requirements. One reference system hardening is carried out in reality. The process consists of implementing security measures and auditing, and it is repeated until the auditing criteria requirements are fulfilled to that extent as required.

Auditing criteria are built to set up the minimum level for the requirements that are set by law, and its purpose is to audit that the requirements are met. In this study one investigates different quidelines and how they can be used to fulfill the requirements of auditing criteria, even if the security requirements were not defined in the procurement contract. This study focuses on evaluation of VAHTI-programme and auditing criteria (A681/2010; A210/2016).

4 Theory background

The word “cyber” was first introduced in 1948 by Norbert Wiener in his book “Cybernetics or Control and Communication in the Animal and the Machine”. Wiener wrote about how machines could someday work without human influence and constant control. He also introduced the term cybernetics, however originally it was translated from ancient Greece, where the term “Kybernetes” was used to describe the control on humans (governor) (Merriam Webster Online dictionary Cybernetics).

In 1982 William Gibson wrote epoch novel “Neuromancer” that really adopted the term “cyberpunk” for wider use (Jenkins, 1997). In the 1990s the term “cyber” was really popular and widely used for many purposes to describe anything from cyberspace to cybersex (Newitz, 2016).

The term “cyber” is used to explain where things take place and happen. This means that cyber domain is used to describe that things do not take place in physical domain and so called real world. Comprehensive security takes into count both cyber and physical world security issues. For example, it is possible to cause distraction to physical world from cyber domain by shutting down heating. It is also possible to distract cyber domain from physical world/domain by closing down power supply from data center. Comprehensive security needs both domains to be taken care of. For a Finnish vocabulary on comprehensive security and explanations on certain words refer to Sanastokeskus (Sanastokeskus 2014:22).

Risks in both domains can be predicted by some factors and it is possible to expand preparedness plans up to imaginary risks. In the scope of this thesis is, however, only about the technical aspect of national security audition criteria part. Risks are simulated by commonly known factors and models used behind best practice models. Because of security classifications it is not possible to use threat models in this thesis.

Certain terminology is commonly used in the field of military information systems. In this study the term ”system” is used to describe the life cycle support models, computer hardware and software that are purchased as a part of certain procurement. Life cycle support models refer to help desk services, updates, upgrades etc. usually including the testing of COTS software updates with custom applications. The system includes life cycle support models that can be either internally produced or outsourced. Computer hardware can be custom designed for intended use or common off the shelf hardware. The software can also be either customized or it can consist of different kinds of CGM applications, where CGM refers to common government military of the shelf.

4.1 Governmental and military business information systems security

In the field of governmental and military business there are several constantly active threats and actors would benefit if security were to be compromised. These threats include e.g. governmental funded actors, military intelligence, activists and hacktivists, to mention a few. The industry tempts all kinds of actors both in peace and crisis.

The military information systems are implemented as a part of a weapon system, a logistics system or another existing need. Military industry has been a pioneer when it comes to protected information. Many requirements, such as information back up, archiving and personnel security are already taken care of.

In the military industry the protected information has different features than protected information, such as product design secret in commercial industry. The product design secret needs to be kept confidential throughout the product design cycle, where protected information confidentiality may expire after mission has been accomplished. On the other hand, the non-repudiation, integrity and availability of knowledge are valued more than in the commercial industry.

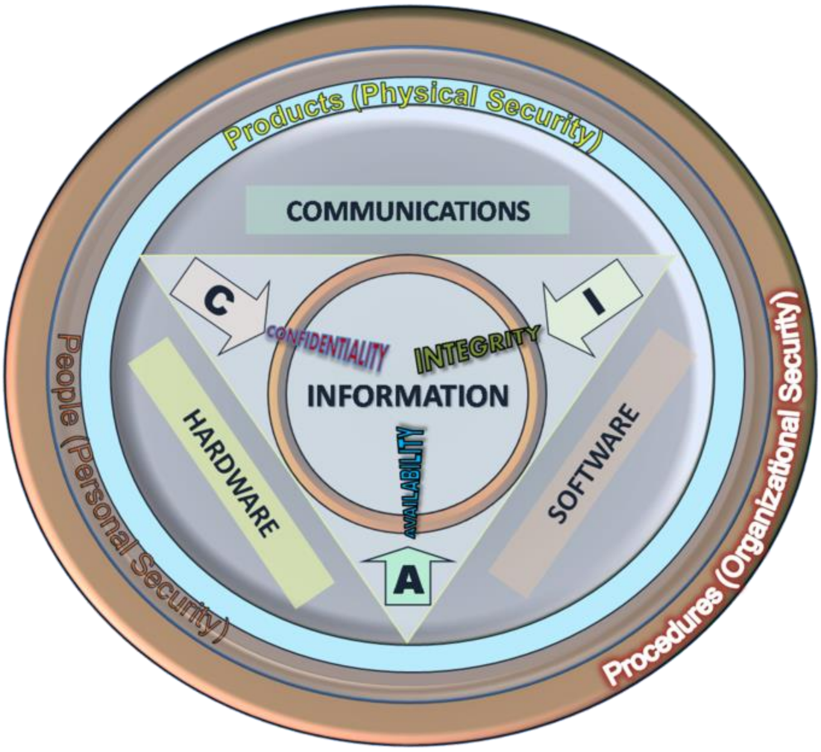

Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
AVAILABILITY
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Figure 1. The Information Security triad (JohnManuel, 2009.)

Availability, integrity and confidentiality are the three main parts of security, and balancing between them is the most important aspect of information security. Information Security Triad is the most commonly used model to describe this balancing. It is also used to help to identify the three main parts and to demonstrate how hardware, software and communications involve information security.

Information Security Triad is the most commonly used model to describe balancing between Confidentiality, Integrity and Availability. It is used to help to identify three main parts of the security and to demonstrate how hardware, software and communications involve information security. Balancing between availability, integrity and confidentiality is the most important aspect of the information security.

> *Confidentiality, Integrity and Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.*

(Wikipedia, 2016.)

4.2 Cyber security threats

One of the most interesting publishing on cyber security field was RUAG´s espionage case. These kinds of cases are not usually published. RUAG´s case is a good example of two things. First, it demonstrates that it is impossible to build sure protection against governmental actor with unlimited resources. Secondly, it is a good example of how long time usage data logging and examination of the anomalies may reveal an APT actor. RUAG´s network was properly hardened against attackers, meaning that security measures were implemented and systems were updated properly. However, all implemented security perimeters were compromised and huge amounts of the data was successfully exfiltrated by an attacker.

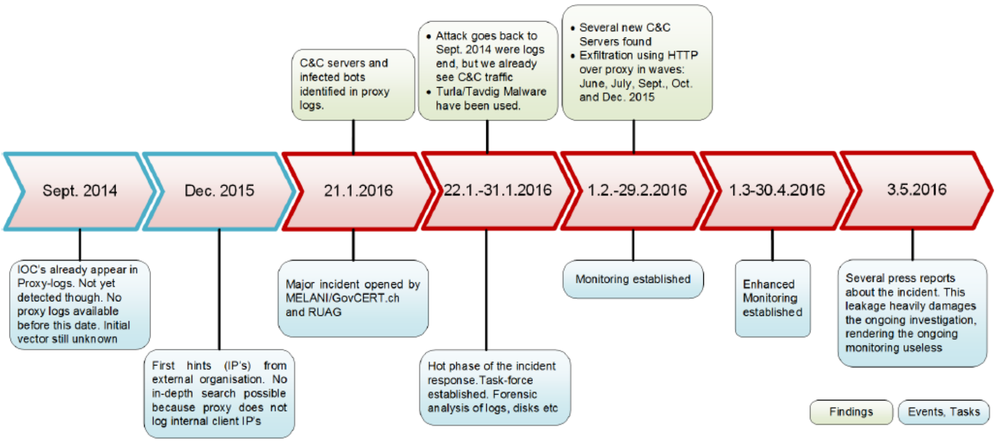

C&C servers and infected bots identified in proxy logs.
• Attack goes back to Sept. 2014 were logs end, but we already see C&C traffic
• Turla/Tavdig Malware have been used.
• Several new C&C Servers found
• Exfiltration using HTTP over proxy in waves: June, July, Sept., Oct. and Dec. 2015
Sept. 2014
Dec. 2015
21.1.2016
22.1.-31.1.2016
1.2.-29.2.2016
1.3-30.4.2016
3.5.2016
IOC's already appear in Proxy-logs. Not yet detected though. No proxy logs available before this date. Initial vector still unknown
First hints (IP's) from external organisation. No in-depth search possible because proxy does not log internal client IP's
Major incident opened by MELANI/GovCERT.ch and RUAG
Hot phase of the incident response. Task-force established. Forensic analysis of logs, disks etc
Monitoring established
Enhanced Monitoring established
Several press reports about the incident. This leakage heavily damages the ongoing investigation, rendering the ongoing monitoring useless
Findings
Events, Tasks

Figure 2, timeline of RUAG case

Timeline of the RUAG case is quite long, and as it can be seen, the malware has been present on the network for a while (MELANI:GovCERT, 2016). Costs of this kind of operation are extremely high. Malware used in APT attacks ate one time only useable and after detection it was almost worthless. Development of the malware itself have taken years. Development of this particular malware was based on Turla family of the malware that has been active since 2004 Over ten years of the active development means that costs for this kind of attacks are millions of euros. Also C&C channels, spreading of the malware and analysis of the exfiltrated data are expensive. Actors who have this kind of resources and who are able and willing to execute this kind of campaigns are active on this field of military information systems. (Symantec Security response, 2014.)

4.3 Development of software suppliers

The original procurement contract can have been made with a company that has evolved in many ways. The name, personnel and ownership of the company may have changed many times during a project. One example of this is Airbus Defence and Space. As the following chart describes, the company has evolved during the last ten years. In 2016 company was again at changing state and Defence and Space will be reorganized at first quarter of 2017 (Airbus DS Electronics and Border Security (EBS), 2016).

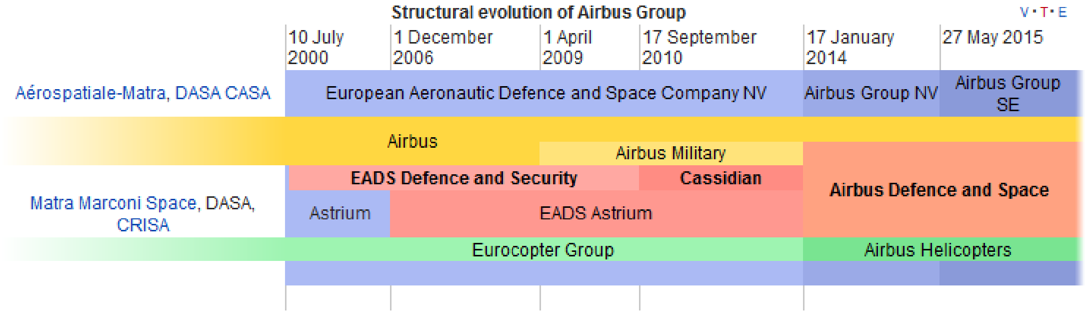


Figure 3. Airbus Defence and Space (Wikipedia, 2016.)

An existing system may have been in operational or testing use already. The system may be already compromised. Vatanen (2015) wrote his thesis on Intrusion Detection During IT Security Audits. Usually, during the new system implementation, all hardware devices are new, as far sealed and secure as possible. There are also requirements that all devices and software should be delivered only by secure companies and personnel. When the security level of an old or existing system is elevated and system is prepared for auditing, it might be the easiest way to fulfill the requirements by discarding all existing hardware, and to install and build new clean instance of complete system.

4.4 Changes in the threat environment

There has been a radical change in the threat environment during the past ten years. Both comprehensive security and the actors causing threats have changed. Hacking has become more professional. After Edward Snowden revealed large scale governmental information gathering, the awareness of activities of other intelligence agencies has raised. Western world intelligence agencies are more publicly known actors. This same kind of change has been going on also in the eastern world. Governmental agencies are recruiting more and more people, which can be seen as a threat as these actors have almost limitless resources of knowledge and money. China, for example has partly publicly admitted that they have a cyber intelligence project going on. (Greenwald, MacAskill and Potras 2013; Harris 2015; FireEye 2016.)

Protected assets are also developed, however, not so much as threats. Information that needs to be protected remains the same and the classification of restricted and secret information has not been updated during the last ten years. Physical security measures of information security assurance are almost the same as ten years ago. Sensitive information is still used as part of operation planning and it needs to be protected. What has changed, however, is the way this information is used. Information has to be accessible and authentic. As an example, airspace coordination order (ACO) needs to be distributed for many different systems and all those environments must get that information in order for the authenticity to be guaranteed. US Airforce LeMay Center for Doctrine Development and Education defines information security perimeters for ACO´s as follows (US Airforce LeMay Center for Doctrine Development and Education, 2014.):

> *Effective airspace control means securing the systems enabling that control. The systems comprising our airspace control system include, but are not limited to, sensors, communications, data processing, and common operating databases. Information assurance programs such as communications security, physical security, emissions security, and network defense are methods to protect airspace control systems and information. Due to the US military's dependence on and the general vulnerability of electronic information and its supporting systems,information assurance is essential to airspace control. Additionally, when developing communication policies and procedures, it is imperative operations security (OPSEC) practicesare applied.*

5 Methods

The study is a qualitative case study. The research question to be answered is how protecting an existing system, where security measures can no longer be built inside the system. differs from a new system, where security controls can be added directly into the system during development and implementation. A question to be answered is whether it is possible to pack the unprotected unsafe system with the help of other security controls in a way that it creates a safe system? Also, if the system cannot be updated, what does it mean as far as the risks are concerned, especially if one has tried to protect the system by external means.

5.1 Case 1, Is it possible to build protection rings and onion model security on an existing system

National Security Auditing Criteria has one specific question regarding counter measures for malware defences. KATAKRI (2015: 47) describes how antimalware software can be left out if a scanning point is established and imported information is sanitized before it is transferred to the protected system(KATAKRI 2015, chapter I9, page 47):

> *Torjuntaohjelmistot voidaan jättää asentamatta ympäristöissä, joihin haittaohjelmien pääsy on muuten estetty (esim. järjestelmät, joissa ei ole mitään tiedon tuonti-/vientiliittymiä, tai joissa tarkasti rajatuissa liittymissä toteutetaan siirrettävän tiedon luotettava validointi/sanitointi).*

Also a requirement of keeping a certain log of classified documents is included in the criteria. This logging requirement is only for classified information that is inserted into the system (KATAKRI 2015, chapter I 18 page 59). Requirements to keep classified data safe do not only mean that it should not leak out, but that it is also to be kept confident, integriable and available.

Information flow from internet to secure environment may be implemented in following way:

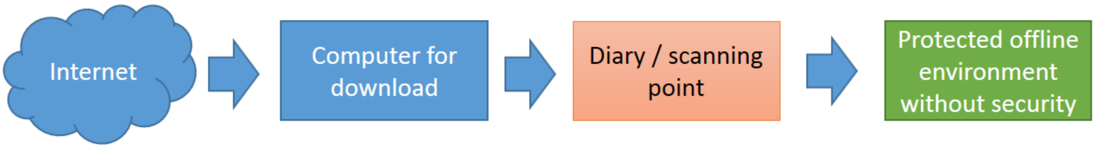


Figure 4. Information flow from unsecure sources to protected environment.

In this case it is assumed that data transfers are safe one way only, and they do not posses a risk of data leakage and loss of confidentiality. There still remains the risk of malware leaking from unsafe sources into the protected environment and causing the loss of data availability or integrity. In some cases, non-repudiation of classified data is an even more important asset to protect than the confidentiality or availability of the data in mission planning systems or similar uses, where information is used as a base for critical decision making.

In this case it is assessed whether it is possible to fulfill requirements by simply creating a scanning point for inserted data, and how safe it is to scan imported data with a commonly used antimalware solution. There is a known risk that fingerprint or heuristics based analysis detects only previously known malware, and does not detect completely new samples or samples which are only used once. This risk is usually accepted, and therefore not taken into consideration during this case. Therefore, for example, sandboxing will not be implemented.

5.2 Case 2, What kind of risks might be realized when system updates are not possible and system is not monitored

The second case in this thesis concerns the updating of a system and the monitoring of system events. Information security is based on the OODA loop model where constanly updated threats and vulnerabilities are inspected and the system is constanly checked for marks of security incidents and the system administration reacts and implements counter measures against realized security events.

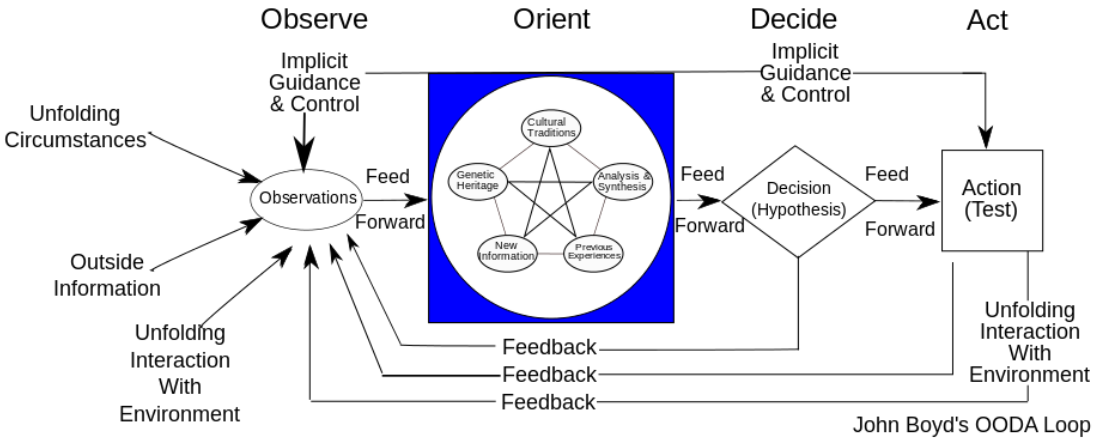


Figure 5. OODA-loop (Moran,P. 2008. John Boyd's OODA loop)

OODA loop refers to constant Observation Orientation, Decision making and Acting for external and internal security events (Moran, 2008). These events can be the released updates of the security patches from the software vendor, log entries showing a problem in the system or anything that can affect system security.

The continuous improvement of the system includes constant checks of the system, clear implemented processes for checking available patches and updating the system. If one of these steps is missing it might break the OODA loop of the processes. This case aims to assess the effects on system security and the ideology of the continuous improvement of system security in a situation where the upating system is left out of the process.

5.3 Case 3, If system has been implemented beforehand, what aspects of system security should be considered

If the system has been implemented beforehand, there are several different vectors that should be taken into consideration. Firstly, if the system has been implemented and has been in use, there is the risk that the system has been comporomised before security measures were implemented. Secondly, there is also the risk that some active APT or malware already exists in the system that cannot be detected by simple scans. This is, however, left out of consideration in this thesis and this has been already investigated by Vatanen in his thesis (Vatanen 2014).

In this case it is investigated which risks remain, even if the system is installed into a completely new eviroment with sealed and secure hardware. If the system has previously been in use, and installation instructions for the system exist, the installation scripts and system have been used by several users over a long period of time leading to many differend kinds of security issues being realized. Complex systems are usually installed partly by automated scripts and partly manually.

If installation scripts or installation instructions have been used for a long time, there may still remain the possibility of them having been leaked. Software providers usually want to sell their products to as many customers as possible, and with as minimal changes as possible. Software releases also include usually some kind of installation instructions and documentation. Documentation is also copied for other customers. Government funded projects also have some publicity requirements, requiring that some documents are publiced on purpose to wide audiences. Patents are also publicly available information and so on. These factors lead to a great deal of design information and instructional information possibly already being public.

As an example, if the system has always been installed with some simple passwords and those passwords are commonly known due to them possibly remaining in the installation instructions or in scripts, a clear security issue is posed due to the insecurity of the passwords. Main question of this case is, what are the ways of regonizing and identifying these security risks posed by the information which remains available to outside entities and beyond the control of the entity responsible for the implementation of the system before the system is implemented in a clean new environment.

6 Research results

6.1 Case 1, How additional protection rings and security check points performed

Limiting access to the system can be seen as consisting of many layers. The physical layer controls are usually required from systems with higher security clearance. Systems with higher than national restricted security level are not permitted to have any connection to the public Internet and people with access to these systems should have security clearance. Some data must be updated from unsafe sources and it must be inserted into the system. For example, a weather forecast is published on the Internet and it is transferred after checking to the secure system. There also remains the risk of losing the physical control over a workstation or an entire system. In any case, there should be security measures in place to prevent catastrophic failures as these risks may realize.

6.1.1 Limiting open interfaces to the workstation

Limiting open interfaces to the workstation can be seen as a basis for hardening. One should have a minimum amount of external interfaces to workstations. The portable work stations, that may also be used in unprotected areas, have to be protected in a way that prevents any catastrophic failures from happening, even if they were to end up in wrong hands. Small, but important measures can be taken to protect the data in work stations. Firstly, the data should be kept minimal. Secondly, it should be made sure that opening the work stations without credentials takes enough time, so that the security of the operation is not compromised. Thirdly, opening the work station should be so demanding that other than operators funded by governmental entities cannot do it with their limited resources. Figure 6 illustrates open interfaces in server client environment. Every interface poses a risk.

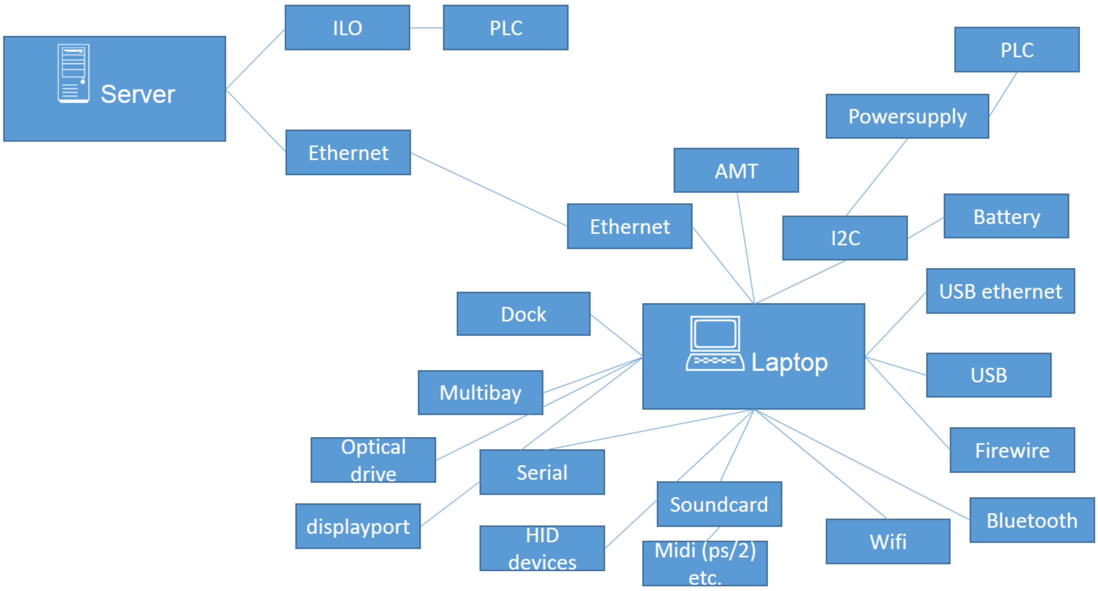


Figure 6. Simplified model of external interfaces.

External interfaces of the system can be illustrated in different ways. Simplified air capped network model can be drawn as figure above shows. The server is shown only as a simplified model without external connections. This is because the server can be protected and isolated with virtualization solutions and by controlling physical access to the server.

One interface of the server is taken under closer consideration. Power line communication links are not widely seen as external interfaces, even if they exist as a default in new server hardware. Power line communications can be seen as a breach of the protection layer based on physical isolation. Servers and network devices with different security classifications may be located nearby in racks. Uncontrolled communication channels between different security classification devices should not exist.

For example, HP has PLC communication capable power supplies in their new line of the servers. These features have been on the market for the last 6 years, and there is a Platinum series of power supplies which are installed in many facilities. Some of these power supplies require special cables and do not use home PNA kind of power line modulated signals for data transfers. In the case of HP, these PLC communication devices use HP ILO (Integrated Lights Out) module of the server. An ILO module is a separate integrated computer inside the server, which runs a protection ring below operating system. The ILO module can control the server power supply and read out various data from the operating system. ILO software is a tiny ARM based proprietary operating system that can be audited only as a black box. PLC communication is used between servers and infrastructure hardware like rack cabinets for server power distribution, cooling management and server identification.

> *HP Common Slot Platinum and Platinum Plus Power Supplies include an embedded power line communication (PLC) feature that allows the power supply to communicate server data (such as server name, UUID, and IP address) to an HP Intelligent Power Distribution Unit (iPDU). This feature is supported on most HP ProLiant G6 and G7 servers that support HP Common Slot Platinum power supplies, as well as on new HP ProLiant Generation 8 servers supporting HP Common Slot Platinum Plus Power Supply options.*

(QuickSpecks Overview, HP Common Slop Power Supplies, 2015)

Figure X illustrates interfaces grouped by possibilities for access limitations.

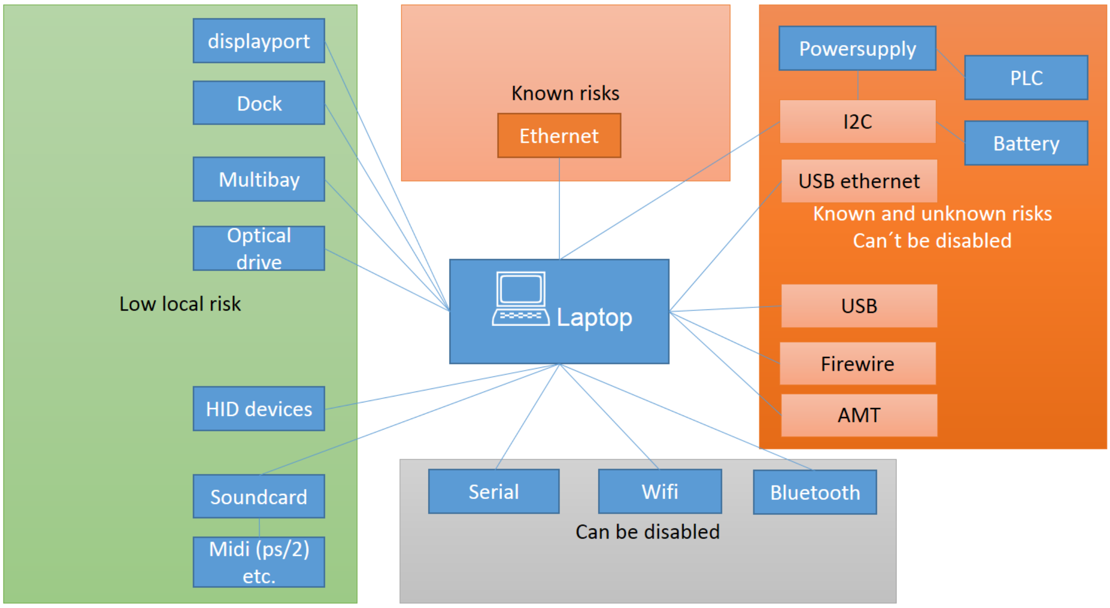


Figure 7 Simplified model how only certain interfaces can be disabled.

The external connections of the work stations can be limited either by cutting them out totally or by restricting communications that run through the interface of the work stations. Usually it is possible to completely remove wireless interfaces from the system. This can be done by simply removing physical wireless communication devices. Other interfaces are much harder to disable or remove completely. Interfaces are either needed or cannot be removed.

Low risk local interfaces are needed for a user to be able to access resources on a computer. Multibay or an equivalent interface is usually a SATA interface for a hard disk, but it may contain an i2c bus intefrace or another interface for battery. Display port is a bidirectional interface, but there have not been publicly known working exploits for that. Optical drive HID devices and soundcards can be used to infect a system, but the risk remains low as long as user accounts are not compromised.

High risk interfaces such as Firewire, USB, USB Ethernet etc. are known to be exploitable to bypass security measures. USB and Firewire interfaces can be used to read out memory from a running computer even if the computer is locked. Microsoft (Microsoft article ID 2516445, 2014) has released instructions for how to block one simple attack vector by adding a group policy that prevents the installation of the two devices used to exploit the DMA vulnerability.

> *A BitLocker-protected computer may be vulnerable to Direct Memory Access (DMA) attacks when the computer is turned on or is in the Standby power state. This includes when the desktop is locked.*
>
> *BitLocker with TPM-only authentication lets a computer to enter the power-on state without any pre-boot authentication. Therefore, an attacker may be able to perform DMA attacks.*
>
> *In these configurations, an attacker may be able to search for BitLocker encryption keys in system memory by spoofing the SBP-2 hardware ID by using an attacking device that is plugged into a 1394 port. Alternatively, an active Thunderbolt port also provides access to system memory to perform an attack.*

(Microsoft article ID 2516445, 2014).

Microsoft (Microsoft article ID 2516445, 2014) recommended resolution for this is:

> *Some configurations of BitLocker can reduce the risk of this kind of attack. The TPM+PIN, TPM+USB, and TPM+PIN+USB protectors reduce the effect of DMA attacks when computers do not use sleep mode (suspend to RAM). If your organization allows for TPM-only protectors or supports computers in sleep mode, we recommend that you block the Windows SBP-2 driver and all Thunderbolt controllers to reduce the risk of DMA attacks.*

6.1.2 Least privilege principle and hardening

Least privilege is a basic method behind the ideology of the hardening in this case. Everything that is not necessary for completing the job should be blocked out and closed. As these military information systems for operational use are usually built for one reason and one use only, there are a lot of useless and harmful standard features that exist in CGM and COTS software and hardware. Computer hardware is built to be usable in as many ways as possible and there are open interfaces of all kinds. Most of the open interfaces are not needed and network protocols and bundled software may just create security concerns or harm to the system.

> *"Least privilege is a foundation principle for information. It needs to be applied to all aspects of information security at your enterprise. Since proper application is so widespread and diverse, many different parts of the organization can make or break its application. The principle of least privilege has a direct dependence of other foundation principles, as well as, a dependence on well-accepted control processes. Proper application of the principle requires an initial investment and an ongoing discipline on the part of all management and staff at an organization. The examples of modern operating systems demonstrate that the responsibility even extends to vendors outside the organization. "*

(SANS Institute, 2003, 17.)

In this case the threat is an imaginary situation where a workstation has been lost. A full set of the National Auditing Criteria is not met. As the basic threat in this case is a situation where a workstation, or more precisely a laptop, is lost and everything within it is now in the hands of a possible evil entity. This study aims to show what counter measures should be in place for the minimum protection to be met.

A list of a basic hardening set:

- Full disk encryption
- Disk locked with ATA lock or similar
- Trusted Platform Module
- Intel Active Management Technology (AMT)
- Firewire and USB DMA protection
- RDP and other remote usage protocols disabled
- Local Firewall enabled
- User Accounts with sufficient passwords and lockout policies
- Bios Protected by a password

Disk Encryption is the basis of all the other counter measures. A national list of accepted encryption devices and software is maintained by NCSA (Viestintävirasto 238/651/2013/2016). Bitlocker is not on this list, and if Bitlocker is used, it should be taken into consideration that at least the older versions of Bitlocker were vulnerable. At this time there are open issues with Bitlocker, and if Bitlocker encryption is used, then systems should be updated regularly and it should not be trusted. Nabeel has introduced two new vulnerabilities in Bitlocker and only one is fixed at this time (Nabeel, 2016).

Bitlocker uses a Trusted Platform Module (TPM) chip that is usually connected to the Intel Active Management Engine AMT. Even TPM and Management Engine are not strictly tied to each other, usually the chipset's own TPM module is connected to the AMT. For example, Lenovo has integrated TPM and other TPM chip on the motherboard. This is mainly because of the different TPM versions, but it might be also built to bypass the possibility for backdoor access to the TPM. Intel is currently one of the two vendors for enterprise workstation chipsets on the market. There is AMT technology present in almost all of the usable laptops. AMT technology runs inside the new Intel CPUs and it has its own real time operating system. AMT is another computer inside the computer as Integrated Lights Out modules are, but

AMT uses RING -3 level and it is able to bypass all the security controls of the operating system. AMT technology has its own access to the network connection that bypasses all the firewalls and operating system level settings. Because of this and the security concerns present in the AMT itself there is a chance that every system including Intel chipset has a backdoor ready for use that can be used by governmental actors. Rutkowska (2015) has published a credible writing about TMP and AMT security issues.

In this example USB connections are vital for the system itself and it is not possible to remove them completely, as described in chapter 6.1.1. USB poses also another kind of a risk, as there are other than basic USB device connection. Ethernet over USB is a device class that is not a regular USB device that needs drivers and installs into the Windows environment as a new USB device. Ethernet over USB devices are simple USB devices that use the electrical connectivity of the USB port and work like Ethernet adapters. This opens a new kind of an attack vector that was introduced in 2016 under the name Poisontap Samy Kamkar (Kamkar, 2016). An Ethernet over USB attack is dangerous because it opens a new network interface and broadens the surface for possible attack vectors (Wikipedia: Ethernet over USB, 2016).

Remote access to the workstation should be limited to the minimum. It would be the best solution, if all the incoming network traffic were to be blocked by a firewall. A firewall is mandatory, not only for blocking remote attacks over the Internet, but also to block local exploits in case physical control to the device is lost. RDP, telnet, SSH and other remotely useable services provide ways to exploit workstation locally.

Any open interface means that a local attacker may gain access to the system by exploiting its weaknessess. The are several ways to exploit the local interfaces. For example, one local attack against phones was based on a brute force key code attack. There was a reset button hardwired to the circuit board of the phone. This worked because the phones marked failed login attempts only after giving a message to the user. By doing this the attacker gained unlimited attempts to breach the key code and was able to unlock the devices. Another, a more sophisticated way, was to remove the flash chip from iPhone devices. The local attacker made cloned, exact, copies of the chip. Failed key code attempts locked out the phones. The attacker replaced the locked copies of the chips with fresh ones and repeated this as many times as it was necessary in order to unlock the phones. (Skorobogatov, 2016.)

National security auditing criteria 2015 chapters I08 and I15 (KATAKRI 2015) describe that all wireless communication must be regarded as a public network. If the protected, isolated, information system does not meet the minimum requirements for communication encryption, firewalling and hardening, then the easiest way is to remove all wireless communications. Removal of the wireless communication hardware is the most secure way to mitigate the risk of the air capped network exposure to the public network.

National security auditing criteria 2015 chapter I08(KATAKRI 2015) describes that infrastructure should have necessary limitations and access control. All network devices, processes and shared directories should have their access limitations set to the strictest settings possible. There is also one separately mentioned clause that autorun, autoplay and automatic startup of all possibly vulnerable software and documents should be prevented from external media. Automatic driver installation of external devices should also be prevented when the workstation is locked. Bios settings should have a password protection. All these counter measures are designed to minimize the open interfaces to locked workstations.

In the national security auditing criteria 2015 chapter I08 (KATAKRI 2015), there is also a requirement to enable the operating system’s own security enhancements. Data Execution Prevention (DEP), Address Space Layout Randimization (ASLR), Applocker and SELINUX are mentioned separately. There are some limitations to the usage of these techniques. Software vendors may not permit the usage of these because systems themselves are not tested and approved in the environment where they exist. Military information systems may have decades long development periods and therefore there exist underlying software components that still use Windows XP era libraries.

Enhanced Mitigation Experience Toolkit (EMET) is a useful software to simplify the turning on of different hardening options in a Microsoft Windows environment. With older systems, these hardening options usually cause multiple problems. Older systems may, for example, require write access rights to the program folder for users, and this is prevented by default. Also, direct device access is not preferred anymore as it was with Windows XP and older systems.

Code signing could be one solution in air capped environments. Another useful technology for hardening is to simply implement checksum calculations and the search for discrepancies during system operation. Distribution of certificates, the comparing of modified files, the search for harmful modifications and discrepancies among normal usage model based file modifications require a lot of work.

6.1.3 Problems in this model

If the system is completely isolated from external networks and all external interfaces are protected, there still remains the need to import external data from untrusted sources. External data can be imported to isolated environment using separate scanning point. One particular test was conducted during the thesis to demonstrate how vulnerable this model is and how easily this model is compromised.

National audition criterion, chapter I9 (KATAKRI, 2015) describes that it is not necessary to install ”defensive software”, if all input data for system is already scanned. When a scanning point is set up and all data is scanned, the question remains, how can system administrators be certain that all the inserted data really is scanned, and how is it possible to get malicious software past that scanning.

Virus detection systems can be divided to 6 different categories:

- Signature detection
- Emulator and Sandboxing
- Heuristic detection
- Behavioral detection
- Proactive detection
- Host intrusion prevention and detection systems (HIPS/HIDS)

Signature detection systems are the oldest and most traditional systems. With Signature based systems there is always the particular challenge that someone must have already previously performed the detection and created a signature for the threat before it can be detected. Signature based system have good detection ratio for known files. Advanced, one time only useable malware files cannot be detected with this technology. Most gateways and static file scanners are based on this technology. Scanning may also include reputation scanning, which means that scanned files external sources are checked for popularity and other values in order to make a decision about the reliability of the file.

Emulator and sandboxing technology is an advanced detection system that attempts to run suspected executable files in an isolated and protected environment. In that environment the file is executed and the acts carried out by the file are analyzed. If the file triggers some suspicious activity it causes an alarm. This technology is time consuming and detects only malicious files that can be run with selected environment specifications.

Figure X illustrates detection capability and complexity in virus detection systems. Heuristic detection software uses complex algorithms to detect malicious software by detecting previously unknown pieces and traces of a suspicious code. Behavioral detection means that software and the environment itself is under constant monitoring. HIDS and HIPS systems usually collect traces of any changes made to the system, files, registry and file checksums etc.

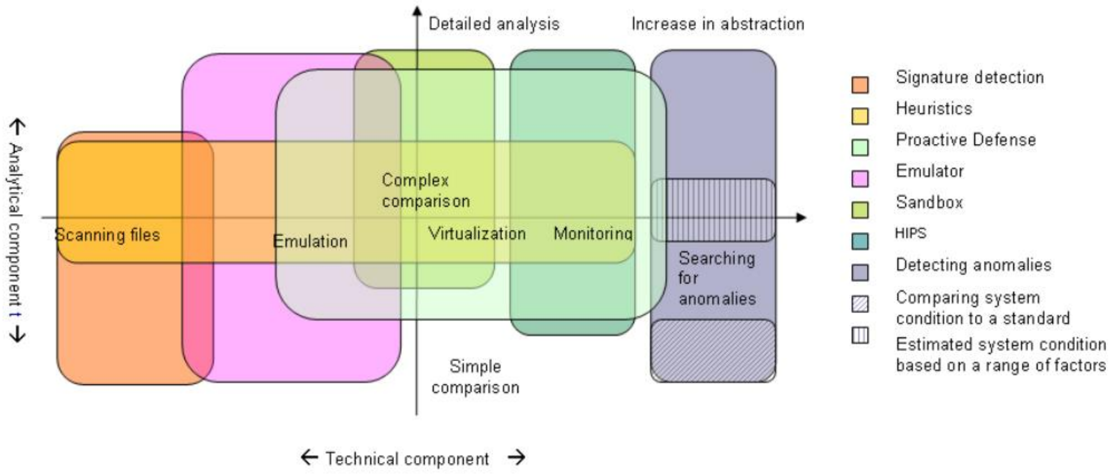


Figure 8. A Model for Assessing Methods of Detecting Malicious Code (Sevchenko, 2008.)

Signature based detection and heuristic detection are the most widely used technologies in scanning workstations in isolated environments. All the scanner engines, however, need to get access to the files that need to be inspected. Encryption protocols like https must be decrypted in a gateway for successfully scan files that are transferred. All archived data should also be extracted for scanning.

F-Secure is a Finnish cyber security company that provides products widely used by most Finnish companies and governmental entities. F-Secure uses their own scanning engines and scanning engines based on Microsoft technology. F-Secure's signature based detection system seems to share some components with Microsoft's technology and the Heuristic, so called DeepGuard technology, seems to be more their own development.

This one particular test was set up with F-Secure and the test setup was built in order to meet the requirements set in National Security Auditing Criteria chapter I9 (KATAKRI, 2015) for separate trusted scanning points for imported data. In this test there are input files containing known test files called EICAR that are built for antivirus software testing. EICAR files have signatures that should trigger a virus detection without any real threat to the system. All F-Secure antivirus products are able to detect these by default.

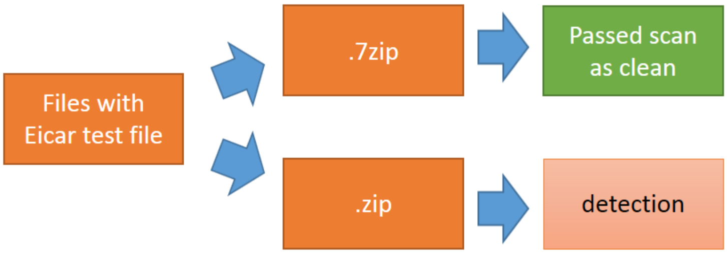
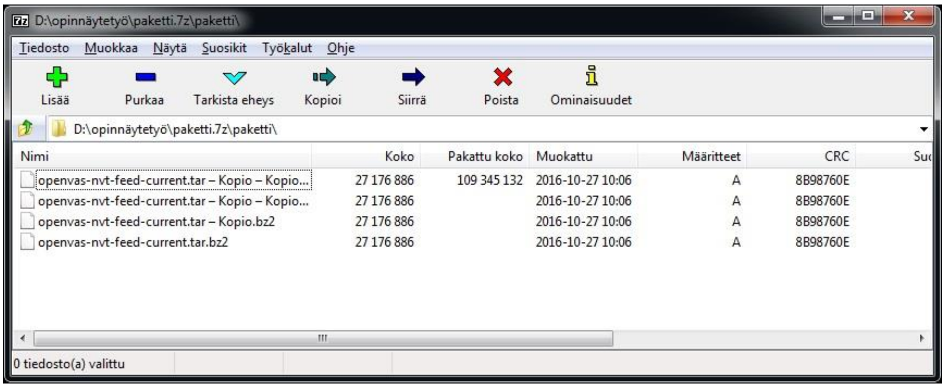


Figure 9. Test procedure.

One vulnerability was found during the testing phase. When files were scanned on the scanning workstation, file numbers did not match the amount there should have been. The scanning engine was able to scan extracted files without problems, however, when files were archived using a 7zip LZMA algorithm F-Secure was unable to open the archives and scan the files.

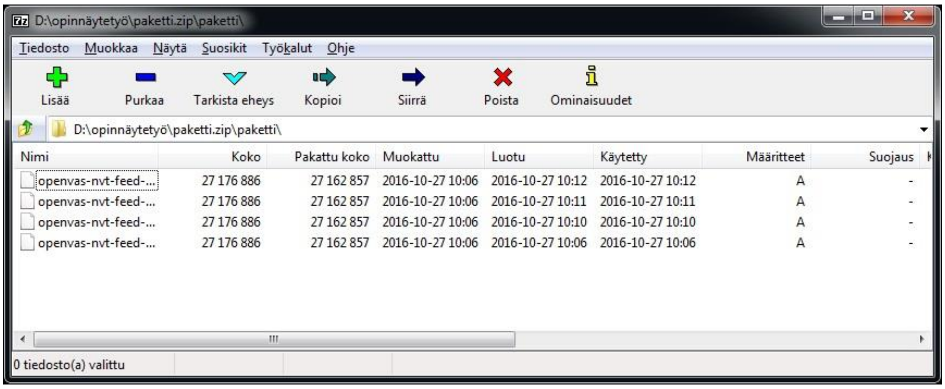
Same files were archived in both 7zip and in zip archive.


D:\opinnäytetyö\paketti.7z\paketti\
Tiedosto Muokkaa Näytä Suosikit Työkalut Ohje
Lisää
Purkaa
Tarkista eheys
Kopioi
Siirrä
Poista
Ominaisuudet
0 tiedosto(a) valittu

D:\opinnäytetyö\paketti.7z\paketti\

Nimi	Koko	Pakattu koko	Muokattu	Määritteet	CRC	Suc
openvas-nvt-feed-current.tar – Kopio – Kopio...	27 176 886	109 345 132	2016-10-27 10:06	A	8B98760E	
openvas-nvt-feed-current.tar – Kopio – Kopio...	27 176 886		2016-10-27 10:06	A	8B98760E	
openvas-nvt-feed-current.tar – Kopio.bz2	27 176 886		2016-10-27 10:06	A	8B98760E	
openvas-nvt-feed-current.tar.bz2	27 176 886		2016-10-27 10:06	A	8B98760E	

Figure 10. Archived files in 7z package.

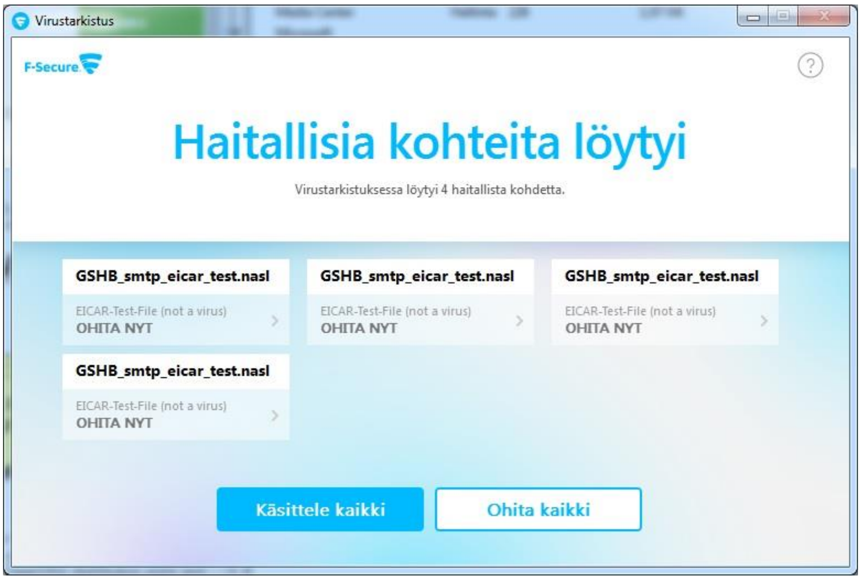

D:\opinnäytetyö\paketti.zip\paketti\
Tiedosto Muokkaa Näytä Suosikit Työkalut Ohje
Lisää
Purkaa
Tarkista eheys
Kopioi
Siirrä
Poista
Ominaisuudet
0 tiedosto(a) valittu

D:\opinnäytetyö\paketti.zip\paketti\

Nimi	Koko	Pakattu koko	Muokattu	Luotu	Käytetty	Määritteet	Suojaus
openvas-nvt-feed-...	27 176 886	27 162 857	2016-10-27 10:06	2016-10-27 10:12	2016-10-27 10:12	A	-
openvas-nvt-feed-...	27 176 886	27 162 857	2016-10-27 10:06	2016-10-27 10:11	2016-10-27 10:11	A	-
openvas-nvt-feed-...	27 176 886	27 162 857	2016-10-27 10:06	2016-10-27 10:10	2016-10-27 10:10	A	-
openvas-nvt-feed-...	27 176 886	27 162 857	2016-10-27 10:06	2016-10-27 10:06	2016-10-27 10:06	A	-

Figure 11. Archived files in zip package.

Files used for the test were OpenVas NVT feed update files. Files that include EICAR test files are large enough to demonstrate this behavior in the F-Secure scanning engine. The same folder was archived into both 7zip and zip format in order to demonstrate the behavior of the scanner engine in this example.



Haitallisia kohteita löytyi

Virustarkistuksessa löytyi 4 haitallista kohdetta.

GSHB_smtp_eicar_test.nasl
EICAR-Test-File (not a virus)
OHITA NYT

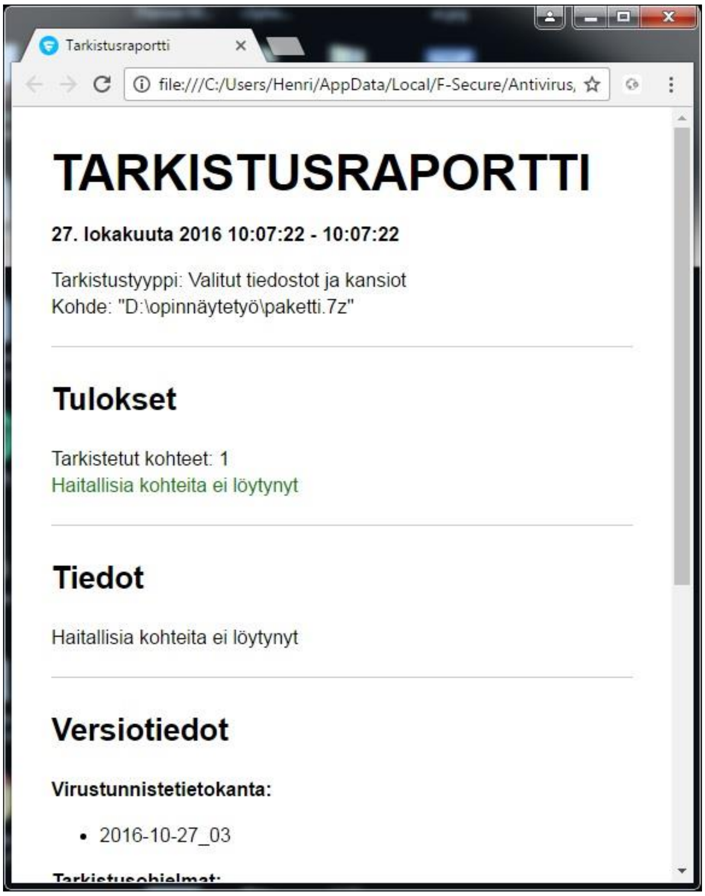
GSHB_smtp_eicar_test.nasl
EICAR-Test-File (not a virus)
OHITA NYT

GSHB_smtp_eicar_test.nasl
EICAR-Test-File (not a virus)
OHITA NYT

GSHB_smtp_eicar_test.nasl
EICAR-Test-File (not a virus)
OHITA NYT

Figure 12. Scanning result of the zip package.

When an archive including files in zip format is scanned, the F-Secure finds the EICAR test files properly.



TARKISTUSRAPORTTI

27. lokakuuta 2016 10:07:22 - 10:07:22

Tarkistustyyppi: Valitut tiedostot ja kansiot
Kohde: "D:\opinnäytetyö\paketti.7z"

Tulokset

Tarkistetut kohteet: 1
Haitallisia kohteita ei löytynyt

Tiedot

Haitallisia kohteita ei löytynyt

Versiotiedot

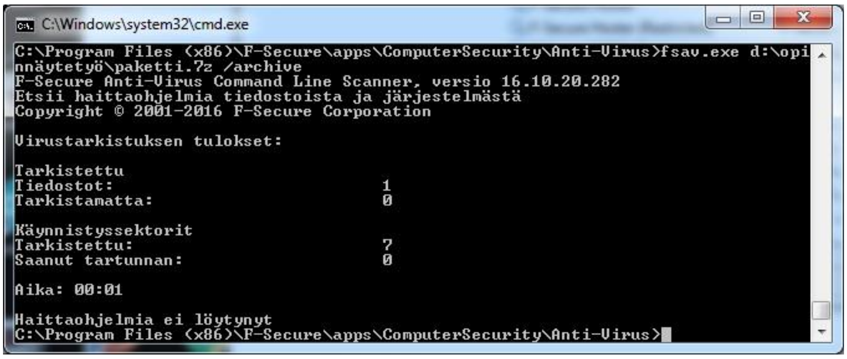
Virustunnistetietokanta:

- 2016-10-27_03

Tarkistusohjelmat:

Figure 13. Scaning results of 7zip package.

When the same files are scanned in 7zip archived package, F-Secure was unable to scan the archive, but reported that one file was clean.



```
C:\Program Files (x86)\F-Secure\apps\ComputerSecurity\Anti-Virus>fsav.exe d:\opi
nnäytetyö\paketti.7z /archive
F-Secure Anti-Virus Command Line Scanner, versio 16.10.20.282
Etsii haittaohjelmia tiedostoista ja järjestelmästä
Copyright © 2001-2016 F-Secure Corporation

Virustarkistuksen tulokset:

Tarkistettu
Tiedostot:                           1
Tarkistamatta:                       0

Käynnistyssektorit
Tarkistettu:                         7
Saanut tartunnan:                    0

Aika: 00:01

Haittaohjelmia ei löytynyt
C:\Program Files (x86)\F-Secure\apps\ComputerSecurity\Anti-Virus>
```

Figure 14. FSAV command line tool forced to scan inside 7zip package.

When a 7zip archive was scanned with command line tool included with F-Secure, it reported that one file was scanned, no files were skipped and nothing suspicious was found. This short and simple test was a demonstration on how easy it is to bypass antimalware scanning software. Bypassing the F-Secure scan did not require any complicated encryption software. Full scan report of the 7zip scan is included in the Appendix 1. F-Secure scanning results for 7z file.

The behavior was found in F-Secure earlier in 2016, and it was reported by F-Secure as fixed within a 6.6.2016 update. A fix for 7zip file scanning did not fix this behavior completely, since there still remains a lack of user response to how the scanning results should be handled. If the scanning of files takes place only at a scanning point and not in a protected environment, and there is no antimalware software installed, then these skipped files marked as clean are a threat. F-Secure describes that a filesystem scanning feature is divided into on demand scanning (ODS) and on access scanning (OAS) (F-Secure, 2016).

F-Secure stated that on demand scanning is designed to skip some files based on file size and calculated scanning time to ensure scanning performance. On demand scanning started manually by a user or on schedule skips these files as it predicts the scanning time to be too long and for the scanning to slow the system down too much. On access scanning is designed to scan all files after extraction.

National Cyber Security Centre Finland (NCSC-FI) was informed that F-Secure products give the user indication that scanned files are clean and instructions on how to demonstrate this as were included in this case. NCSC-FI was able to reproduce this and they opened a ticket for this task. Hopefully there will be some clear indication for the user in future that all the files were not scanned. NCSC-FI also replied that authors behind KATAKRI will be informed.

6.2 Case 2, System was not updated and constantly monitored, what risks the system was exposed to

6.2.1 System updates cannot be installed

Military information systems involving aviation use usually have multi step quality and flight worthiness acceptance tests. System acceptance tests have strictly defined limitations and the updating of the system without complete test sets is usually impossible. DO-178B (Software Considerations in Airborne Systems and Equipment Certification) is a basic guideline and standard used for flight worthiness acceptance. If DO-178B/C is required for an information system and configuration management of the information system is based on a model derived from that standard it makes system update installations impossible outside of the verification model.

6.2.2 Systems logs are not inspected properly

One of the most important principles in information security assurance is the OODA loop. OODA loop means constant Observation Orientation, Decision making and Acting for external and internal security events. When one part of the loop is broken, the rest of the process is useless. If observation is missing, it is impossible to make any decision and react to any threats. This is the reason why observation of system events and continuous checking of event logs of the system is so important.

System monitoring is the key part of the finding anomalies. Anomalies may signify hardware problems, access log anomalies or anything regarding any part of the system. Almost all parts of the modern information system may be monitored. Monitoring in its simplest form means supervising if all hardware is still in good condition. It may refer to any activity from checking if the LED light is green or red, to reading emails generated by an automatic system once a day and checking if the automatic monitoring system has sent some notification.

The system event monitoring process can be partly automatic, but there still remains a need in some point of the system administration for someone to make decisions and react to alerts generated by automatic systems. There always remains a risk that the administrator works for an evil entity. After Edward Snowden revelations, there were publications about fully automatic information security systems, capable of decision making, being used to replace humans in decision making processes. Federation of American Scientists have released Department of Defense paper of Army Insider Threat Program and Business Insider has more dramatic article about this topic about cutting down human resources in system administration tasks (McHugh, 2013; Allen, 2013).

6.3 Case 3, Previously implemented or procured system was implemented, what happened regarding system security

National Security audition criteria 2015 I13 (KATAKRI 2015) determines that software vendors should implement secure coding principles and software development processes should include checks for vulnerabilities. This does not, however, describe how software development related documents and design information should be handled.

National NH90 software projects can be searched by Google and there are two related software project theses available by Ylinen and Hartikainen, in which the author of this thesis is mentioned, and in which a lot of information about systems used in the NH90 can be extracted. Databus describtions, attached devices and communications between systems can be extracted from the documents and even some images have been removed for security reasons. (Ylinen, 2013;Hartikainen, 2014.)

Classified and secret national information system documentation can also be found from public internet. ILPUC2 and related information systems are usually kept as confidential as it is possible, but information about that system can also be extracted from the public sources. Pro Gradu by Pikkarainen is available at Doria. Pikkarainen

(2013) presents a short describtion of the military systems EVTJ, Iris, Core etc. Publicly available knowledge about networks and user groups may be valueable information for hostile entities. Usually all information about this topic is classied. (Pikkarainen, 2013.)

Custom military software procurement contracts have some limitations and they cannot be sold freely by software vendors. Some software components and documentation are reused in other projects and also sold to other customers. After years have passed and originally classified components with classified documentation have been in use by many customers, some end user or a customer might publish some information that could expose the original concept and vulnerabilities of the system for public.

If the system is not recently reinstalled completely, there is a great risk that old administration user accounts are still present. If there have been Administration accounts that have not been monitored and administration tasks have not been logged, then there is also the risk of all the logs of the system not being consistent. Administrators may have been able to clean out some old incidents and traces of the security events. As Vatanen (2015) writes in his thesis, the inspection of the system logs from previous usage is an important task when system security level is elevated.

Advanced Persistent threats are custom malware software made just for one use or altered from some family of malware software in mean to remain undetected by anti-malware product. APT malware software is custom built software that is designed to bypass security measures of the certain environment. Leaked information of the system may be used by evil entity as design material for APT malware software.

Risks to security in existing systems are not usually caused by malicious software. Misconfiguration of the system is maybe the greatest cause of security risks. Old user accounts that are still present in the system are also one of the greatest causes for security risks. Default Administrator and Guest account names are proposed to be changed in National Security Auditing Criteria 2015 chapter I08. Vatanen (2015: 88) writes about one example describing an old Active Directory domain trust still active in a system, even after that system was supposed to be separated from said domain.

Integrated Lights Out modules may be without configuration and they may have active network connections with a shared physical network port. Network devices like switches may have default passwords still in place. There may be completely unnecessary administrator accounts present in the system. Even the documentation of the system may be publicly available and there may even be default passwords in place.

In a Microsoft Windows environment there is the chance that a software has a service account that has default non expiring passwords. These accounts may be created by a software vendor and automatically created during system installation. There is a principle that a system should be made unfamiliar and unknown also to the software vendor.

National trusted software vendors might end up being sold to any actor in the market. For example Stonesoft was a previously extremely reliable partner for the Finnish Defense Forces and for other companies working with information security. Stonesoft was known for their ability to investigate software vulnerabilities and that company took part in Finnish governmental workgroups for information security development strategy. Stonesoft was sold to Intel as a neutral information security actor and after that it was resold to Raytheon. (Liikenne- ja viestintäministeriö, 2006; Darrow, 2015.)

7 Conclusions

The main research question was how protecting an existing system, where security measures cannot be built inside the system, differs from a new system, where security controls can be incorporated into the system as default. As a result of the research a few greater issues were identified when security controls are implemented into the system afterwards.

The first case involved adding additional security rings to protect the system. Additional security added afterwards may limit the access to the system, however, there always remains some open interfaces and ways to exploit the system. Both new and previously implemented systems have the same kind of remaining risks after implementing the security measures. Open interfaces and losing the physical access of the device are risks with both new and previously implemented system. Security issues are raised if there is a limitation for anti-malware software installation to the target system. With a new system it is usually possible to implement anti-malware software to the system itself, however, with previously implemented software it may be impossible because of the limitations from the software vendor. If the anti-malware software cannot be installed in the target environment, it is not possible to detect security issues taking place when imported data is extracted and used in the environment.

The second case was about risks that may occur, if the system is not updated. With the new system it is usually possible to make a contract for continuous updates. If the system is not updateable, then the continuous development and OODA-loop will also be easily broken. If one part of the OODA-loop (Observation, Orientation, Decision making and Acting) is broken, it affects the functioning of all other parts. For example, if the system updates are not installed, there is no longer need for monitoring available updates and known, published, vulnerabilities. This causes serious damage to the comprehensive security of the system as there are limited ways to detect security incidents and then there are no ways to react if something happens.

The third case concerned risks caused by a previously implemented system and leaked documentation. If the system is newly procured, it is easier to keep track of all publically available information and make contracts limiting all the information usage and publication. There were several documents publicly available on the Internet containing information about classified systems. By combining all the pieces together the hostile entity may gain too much information.

The most significant limitation for this thesis was the lack of knowledge about real threats. The information about threats is either highly classifies, it does not exist, or it is about known realized events. NATO Cooperative Cyber Defense Centre of Excellence (Geersm 2011) has published a study how Sun Tzu´s Art of War still contains usable quotes in cyber warfare.

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.* (Geers, 2011.)

The best known quote from Sun Tzu is introduced in this study and brought into the cyber domain. The same principle exists with threats. For example, it is easy to detect malicious software with the existing recognition patterns, where as previously unknown new threats are difficult to recognize. If one’s own information system environment is not familiar, it is almost impossible to defeat security threats.

During the thesis the author realized that the topic of cyber security covers an enormous number of possible threats, and patterns for defending against them. Therefore, it is not possible to build a comprehensive security model that includes all of the possible counter measures. KATAKRI attempts to cover as many potential threats as possible, and it is a good guideline, if implemented completely and system auditing is done properly. Building up a completely auditable environment is usually too expensive and, consequently, only some chapters of KATAKRI are really implemented. For example, some parts may be left out since they are covered by physical access limitations.

In the light of this thesis, it seems to be impossible to measure, how the system hardening has accomplished if no security incidents have been detected. The realization of real security threats is always an unwanted situation. Training for security incident detection is one important task, and it was realized during the work that it should be implemented in to the training and lifecycle support model. The documentation of the process of how potential security incidents are detected should be a part of the system administration manual. The tasks to search for system events, access logs, anti-malware software logs and alerts should be implemented into the basic system administration task list.

Simulated threats and how the system administration is trained to detect security events were also realized to be a part of the future development. This training can be carried out after the administrators of the system know both their own environment and the security events they are expected to manage, cope with and resolve in the future. Training should incorporate threat models which are as realistic as possible. Using real threat models is, however, a challenging task, as they are kept secret and classified. The technical aspect of the threat is usually possible to be simulated in a training environment without exposing the classified parts of the real threat, such as potential attacker identity and possible advanced custom technologies. It is possible to simulate the similar kind of a detected event during the exercise. There are numerous software products in the market built up just for use in training. JAMK University of Applied Sciences has its own training environment to safely train working as the defending entity under attack using a simulated evil entity. These cyber security exercises should be one part of the secure usage model of a holistic system.

References

A 1.7.2010/681. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Accessed on 10.10.2016. Retrieved from http://www.finlex.fi/fi/laki/ajantasa/2010/20100681#L1P1

A 681/2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Accessed on 10.10.2016. Retrieved from https://www.vahtiohje.fi/web/guest/tietoturvallisuusasetus-tietoturvatasot-ja-muut-viitekehykset

Airbus DS Electronics and Border Security (EBS), 2016. Accessed on 5.12.2016. Retrieved from http://detectandprotect.org/

Allen, J. 2013. The NSA Intends To Fire 90% Of Their System Administrators To Eliminate Future Leaks. Business Insider website. Accessed on 6.12.2016. Retrieved from http://www.businessinsider.com/nsa-firing-sysdadmins-2013-8?r=US&IR=T&IR=T

Darrow, B. 2015. Intel to sell Stonesoft network security unit to Raytheon-Websense. Fortune, 28.10.2015. Accessed on 10.11.2016. Retrieved from http://fortune.com/2015/10/28/intel-sell-stonesoft-raytheon-websense/

Edward Snowden: The Whisleblower behind the NSA surveillance revelations. The Quardian, online publication 11.6.2013. Accessed on 30.10.2016. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Ethernet over USB, 2016. Accessed on 24.11.2016. Retrieved from https://en.wikipedia.org/wiki/Ethernet_over_USB

FireEye 2016 Special report / Red Line Drawn: China recalculates its use of cyber espionage, online publication 11.6.2013. Accessed on 30.10.2016. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf

Functionality of F-Secure virus and spyware scanning. F-Secure website. Accessed on 6.12.2016. Retrieved from https://community.f-secure.com/t5/Common-topics/Functionality-of-F-Secure-virus/ta-p/18314

Geers 2011 Sun Tzu and Cyber War. Cooperative Cyber Defence Centre of Excellence (CCD COE). Accessed on 1.12.2016. Retrieved from War https://ccdcoe.org/sites/default/files/multimedia/pdf/Geers2011_SunTzuandCyberWar.pdf

McHugh, J. 2013. Army Directive 2013-18 (Army Insider Threat Program). Department of Defense. Secretary of the Army, Washington. Accessed on 6.12.2016. Retrieved from https://fas.org/irp/doddir/army/insider.pdf

Microsoft, article ID 2516445, 2014. Blocking the SBP-2 driver and Thunderbolt controllers to reduce 1394 DMA and Thunderbolt DMA threats to BitLocker. Accessed on 18.11.2016. Retrieved from https://support.microsoft.com/en-us/kb/2516445

Greenwald, G.,MacAskill, E. and Potras, L. 2013 The Guardian, online publication 11.6.2013. Accessed on 30.10.2016. Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Hartikainen, E. 2014. NH90 Helikoptereiden moottoreiden syklilaskennan kehittäminen ja elinkaarihallinta. Opinnäytetyö. Lappeenrannan teknillinen yliopisto, teknillinen tiedekunta, konetekniikan koulutusohjelma. Accessed on 10.10.2016. Retrieved from http://www.doria.fi/bitstream/handle/10024/96704/DI-ty%F6_Hartikainen_0352023.pdf;jsessionid=D68A08942F61382D9D7FDCCBB59D2D35?sequence=2

JohnManuel, 2009. The Information Security triad: CIA. Second version. Accessed on 1.12.2016. Retrieved from https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

Jenkins, H. 1997. Media and Imagination: A Short history of American Science Fiction. Accessed on 1.10.2016. Retrieved from http://web.mit.edu/m-i-t/science_fiction/jenkins/jenkins_5.html

Kamkar, 2016. PoisonTap - siphons cookies, exposes internal router & installs web backdoor on locked computers. Accessed on 24.11.2016. Retrieved from https://samy.pl/poisontap/

KATAKRI 2015 Liikenne- ja viestintäministeriö. Tietoturvalliseen yhteiskuntaan: Kansallisen turvallisuusasioiden neuvottelukunnan kertomus valtioneuvostolle. Accessed on 12.10.2016. Retrieved from http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Liikenne- ja viestintäministeriön julkaisuja 93/2005, 31.12.2005. Accessed on 10.11.2016. Retrieved from https://www.lvm.fi/documents/20181/755163/Neuvottelukunnan+raportti.pdf/71dea454-8b9d-4862-881d-f092b1467ba2?version=1.0

MELANI:GovCERT, 2016. Technical Report about the Malware used in the Cyberespionage against RUAG. Accessed on 2.12.2016. Retrieved from https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html

Merriam Webster Online dictionary Cybernetics. Accessed on 10.10.2016. Retrieved from http://www.merriam-webster.com/dictionary/cybernetics

Moran, P.2008. John Boyd's OODA loop. Accessed on 20.11.2016. Retrieved from https://en.wikipedia.org/wiki/OODA_loop#/media/File:OODA.Boyd.svg

Nabeel, A: 2016. From zero to SYSTEM on full disk encrypted Windows system (Part 1). Accessed on 1.12.2016. Retrieved from https://blog.ahmednabeel.com/from-zero-to-system-on-full-disk-encrypted-windows-system/

Newitz, A: 2016. The Bizarre Evolution of the Word "Cyber". Gizmodo news site. Accessed on 10.10.2016. Retrieved from http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487

Pikkarainen, A: 2013. HAJAUTETTUUN RYHMITYKSEEN SOVELTUVA TILANNEKUVA-JÄRJESTELMÄ –NÄKÖKULMANA VIESTIHUOLTOKOMPPANIA. Accessed on 1.12.2016. Retrieved from https://www.doria.fi/bitstream/handle/10024/92271/SM%20764.pdf?sequence=2

QuickSpecks Overview. HP Common Slop Power Supplies. DA 14209 World Wide, Version 6, March 25, 2015. Accessed on 17.11.2016. Retrieved from https://www.hpe.com/h20195/v2/getpdf.aspx/c04111541.pdf?ver=6

Rutkowska, 2015. Intel X86 considered harmful. Accessed on 24.11.2016. Retrieved from https://blog.invisiblethings.org/papers/2015/x86_harmful.pdf

Sanastokeskus TSK, 2014. Kokonaisturvallisuuden sanasto Accessed on 13.11.2016. Retrieved from http://www.spek.fi/loader.aspx?id=1c66e01d-a75e-4a9a-80ec-9816340ce752

SANS InfoSec readig Room: Implementing Least Privilege at Your Enbterprise. SANS Institute, 2003, 17. Accessed on 24.11.2016. Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/implementing-privilege-enterprise-1188

Harris, 2015 The Daily Beast, online publication 11.6.2013. Accessed on 30.10.2016. Retrieved from http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html

Sevchenko, A.2008. Malicious Code Detection technologies. White Paper, Kaspersky Lab. Accessed on 1.12.2016. Retrieved from http://latam.kaspersky.com/sites/default/files/knowledge-center/malicious%20code%20detection%20technologies.pdf

Skorobogatov, S. 2016. The bumpy road towards iPhone 5c NAND mirroring. University of Cambridge, Computer Laboratory. Accessed on 27.11.2016. Retrieved from https://arxiv.org/ftp/arxiv/papers/1609/1609.04327.pdf

Symantec Security Response, 2014. Turla: Spying tool targets governments and diplomats Cyberespionage group uses sophisticated malware to target former Eastern Bloc countries. Accessed on 1.12.2016. Retrieved from https://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

Tietoturvakaari, Information Society code 971/2014 Accessed on 10.10.2016. Retrieved from http://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf

US Airforce LeMay Center for Doctrine Development and Education, 2014, 2. Accessed on 30.10.2016. Retrieved from https://doctrine.af.mil/download.jsp?filename=3-52-D03-AIRSPACE-Cntrl-System.pdf

Vatanen, M. 2014. Intrusion detection during IT security audits. JAMK, Master's degree program in information tehcnology. Technology, communication and transport. Accessed on 14.10.2016. Retrieved from https://www.theseus.fi/xmlui/bitstream/handle/10024/81542/Vatanen_Mikko.pdf?sequence=1

Ylinen, E. 2013. Väylävakoilukyvyn ylläpito ja sen kehittäminen. Opinnäytetyö. Tampere University of Applied Sciences, Kone- ja tuotantotekniikka. Accessed on 10.10.2016. Retrieved from https://publications.theseus.fi/bitstream/handle/10024/63295/Ylinen_Eero.pdf?sequence=1

Viestintävirasto 210/2016 O, Ohje Tietoturvallisuuden arviointilaitoksille. Accessed on 20.10.2016. Retrieved from https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf

Viestintävirasto 238/651/2013/2016, Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut. Accessed on 1.12.2016. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/NCSA_salausratkaisut.pdf

Wikipedia: The history of Airbus Defence and Space. Accessed on 10.10.2016. Retrieved from https://en.wikipedia.org/wiki/Airbus_Defence_and_Space

Wikipedia: Information Security. Accessed on 1.12.2016. Retrieved from https://en.wikipedia.org/wiki/Information_security

Appendices

Appendix 1. F-secure scanning results for 7z file

```
F-Secure Anti-Virus Command Line Scanner, versio 16.10.22.283
Etsii haittaohjelmia tiedostoista ja järjestelmästä
Copyright © 2001-2016 F-Secure Corporation

7. joulukuuta 2016 20:52:24

Komentorivi: d:\opinnäytetyö\paketti.7z /ARCHIVE /LIST
/REPORT=D:\OPINNÄYTETYÖ\TESTIRAPORTTI7Z.TXT /ALL

Työasema: kone

Tarkistusasetukset:
Kohde: d:\opinnäytetyö\paketti.7z
Tarkista kaikki tiedostot
Toiminto:
 Virukset: Vain raportointi
Tarkista pakatut tiedostot: käytössä

Tarkistusohjelmat:
F-Secure Aquarius: 11.00.01, 2016-12-07
F-Secure Hydra: 5.15.154, 2016-12-07
F-Secure Online: 16.15.23, 0-00-00

Virustarkistuksen tulokset:
D:
MBR (0x80)
MBR (0x81)
MBR (0x82)
MBR (0x83)
MBR (0x84)
MBR (0x85)
D:\OPINNÄYTETYÖ\PAKETTI.7Z

Tarkistettu
Tiedostot:                   1

Tulos
Virukset:                    0
Vakoiluohjelmat:             0
Mahdollisesti tartunnan saanut:           0
Riskiohjelma:                0

Toiminnot
Puhdistettu:                 0
Poistettu:                   0
Nimetty uudelleen:           0
Asetettu karanteeniin:                    0

Käynnistyssektorit
Tarkistettu:                 7
Saanut tartunnan:            0
Mahdollisesti tartunnan saanut:           0
Puhdistettu:                 0

Aika: 00:00
```