SECURITY TESTING PROCESS OF BASE STATION CONTROLLER

Mika Törmänen

Thesis
May 2012
Degree Programme in Business Information Systems
Option of Data Network Services

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalveluiden suuntautumisvaihtoehto

TÖRMÄNEN MIKA:
Tukiasemaohjaimen tietoturvatestaus prosessina

Opinnäytetyö 58 sivua, josta liitteitä 7 sivua
Toukokuu 2012

Tavoitteena oli tuottaa Nokia Siemens Networksille yleispätevä materiaali tukiasemaohjainta koskevista tietoturvauhista ja tietoturvan testauksesta. Koska mobiilitietoverkkoihin on teknologisesti tullut suuri muutos pakettipohjaisen tietoliikenteen muodossa, materiaalilla on tarkoitus jakaa tietoa erilaisista uhista testausosaston työntekijöille.

Prosessiosuudessa kuvaillaan koko tietoturvaprosessi vaihe vaiheelta resurssisuunnittelusta tulosten säilömiseen asti. Tietoturvatestausta koskevat erilaiset lailliset rajoitteet, joten nämä kerrotaan lakipykälin ja yrityskohtaisen esimerkin avulla.

Prosessia käsittelevässä osuudessa on esimerkkitapauksena toteutettu tietoturvatestaus kahta esiteltyä työkalua käyttäen testaussuunnitelman pohjalta. Työkalun tuottamia tuloksia on analysoitu yleisellä tasolla. Erilaisia ennaltaehkäiseviä keinoja kuvataan laajasti keskittyen tukiasemaohjaimeen. Monet kuvatuista keinoista pätevät myös yleisiin viestintäverkkoihin.

Asiasanat: viestintäverkot, gsm, tietoturvatestaus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Data Network Services

TÖRMÄNEN MIKA:
Security testing process of base station controller

Bachelor's thesis 58 pages, appendices 7 pages.
May 2012

The goal of the thesis was to create a generic guide about security threats and security testing concerning the base station controller, one of the key elements of telecommunications network.

The thesis work was made for Nokia Siemens Networks to stabilize its security testing process concerning the base station controller. The material can be shared with employees for educational purposes. This general material contains various preventive measures focusing on the base station controller. These measures are also applicable to a general communications network.

A fixed mobile network is changing technologies for transmitting data in the network. This brings about different threats and possibilities.

The testing process is restricted by litigation and local constraints which are described in the process chapter. The whole process is described from the resource planning to storing the produced documentation with a product documentation tool.

A small testing procedure based on the example testing plan was carried out to test the documented process.

Key words: telecommunication networks, gsm, security testing

TABLE OF CONTENTS

ABBREVIATIONS

3GPP	Standardization organization for GSM and third generation technologies
AH	Authentication header
ANSI	American national standards institute
BSC	Base station controller
BSC3i	BSC product which can handle 2000 BTSs
BSS	Base station subsystem is a network segment in GSM network which contains BSCs and BTSs
BTS	Base transceiver station
cell	Radio frequency area where call can be made.
DiffServ	Differentiated services is used for prioritizing data
DoS	Denial of service
DS field	Field in IP packet header which contains QoS value for DiffServ mechanism
E1	ETSI standard for TDM connections, 2.048kbit/s bandwidth
ESP	Encapsulating security payload
ETSI	European telecommunications standards institute
FlexiBSC	BSC product which can handle 4200 BTS sectors
FTP	File transfer protocol, unsecured way to transfer data
GPRS	General packet radio service, slow packet based data service
GSM	Global system for mobile communications
HTTP	Hypertext transfer protocol
HTTP-GET message	HTTP message type which is used for getting data from web server
HTTPS	Secured HTTP
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
IDS	Intrusion detection system
IEEE	Institute of electrical and electronics engineers
IETF	Internet engineering task force
IMSI	International mobile subscriber identity
IP	Internet protocol
IPS	Intrusion prevention system

IPSec	Internet protocol security
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISO	International organization for standardization
ITU-T	International telecommunication union, telecommunication standard department
LTE	Long term evolution, technology for high speed data services in mobile networks
Mac OS X	Apple's operating system for desktop and server computers
MITM	Man in the middle
MPLS	Multiprotocol label switching
MS	Mobile station, mobile phone
MSC	Mobile switching center, routes voice calls and sms.
NASL	Nessus attack scripting language
NED	NSN-based customer documentation tool
NSN	Nokia Siemens Networks
NTP	Network time protocol, unsecured protocol to distribute time in network
OS	Operating system
OSS	Operating subsystem, contains means to operate mobile network
PBX	Business telephone system
PC	Personal computer
PDF	Portable document format
PLMN	Public land mobile network
Pronto	Bug correction request or notification
Q3 interface	Interface which provides management information for OSS
QoS	Quality of service
RAM	Random access memory
RFC	Request for comments, IETF memorandum on Internet standards and protocols
SCTP	Stream control transmission protocol
SFTP	Secure file transfer protocol
SGSN	Serving GPRS Support Node, handles GPRS data packets coming from BSC

Sharenet	Document management solution at NSN
SIT	Secure information technology
spoofing	Intentionally falsified value
SQL	Simple query language, usually umbrella term for database services
SS7	Signaling System No. 7, telephony signaling protocol message family
SSH	Secure shell, encrypted tunnel to transmit data
T1	ANSI standard for TDM connection, 1.544kbit/s bandwidth
TCP	Transmission control protocol, connection-oriented protocol
TCP SYN packet	TCP packet type which indicates requested connection
TDM	Time division multiplexing, old method for data transmission
telco	telecommunication
UDP	User datagram protocol, connectionless protocol
WCDMA	Wideband code division multiple access
Windows IIS server	Microsoft’s HTTP server, Internet information services
VLAN	Virtual local area network
VPN	Virtual private network
VRF	Virtual routing and forwarding

1 INTRODUCTION

Thesis is made for a testing department in Nokia Siemens Networks to guide its security testing process and its testing related employees to educate themselves about packet-based networking in telecommunications network. The education material is concentrating on threats and preventive measures concerning the base station controller.

The education material is relevant because packet-switched transmission is a new-comer in GSM (global system for mobile communications) networks. The migration process from the old circuit-switched transmission technology to the new packet-switched transmission raises different threats against the BSC (base station controller).

The telecommunications network is considered high availability network so it must function always. Therefore the threats must be tested regularly.

There are several testing tools which can be used for testing the vulnerabilities. The port scanners are used to probe open ports and gather platform information for the attack planning. Vulnerabilities can be scanned with several different tools which have different features regarding the scanned vulnerabilities and output reports.

The tested BSC belongs to GSM network segment. Threats and preventive measures are mainly concerning the base station controller.

The client company is multinational mobile network technology developer. Its business contains both hardware and software products. Hardware is provided to wide variety of technologies starting from GSM to high end LTE (long term evolution).

2 GSM NETWORK

According to Andreas F. Molisch (2011) the fixed GSM network in Figure 1 consists of three different subsystems where each one of the subsystems provides different services to the network. The three subsystems of the GSM network are

- BSS (base station subsystem)
- NSS (network switching subsystem)
- OSS (operation support subsystem)

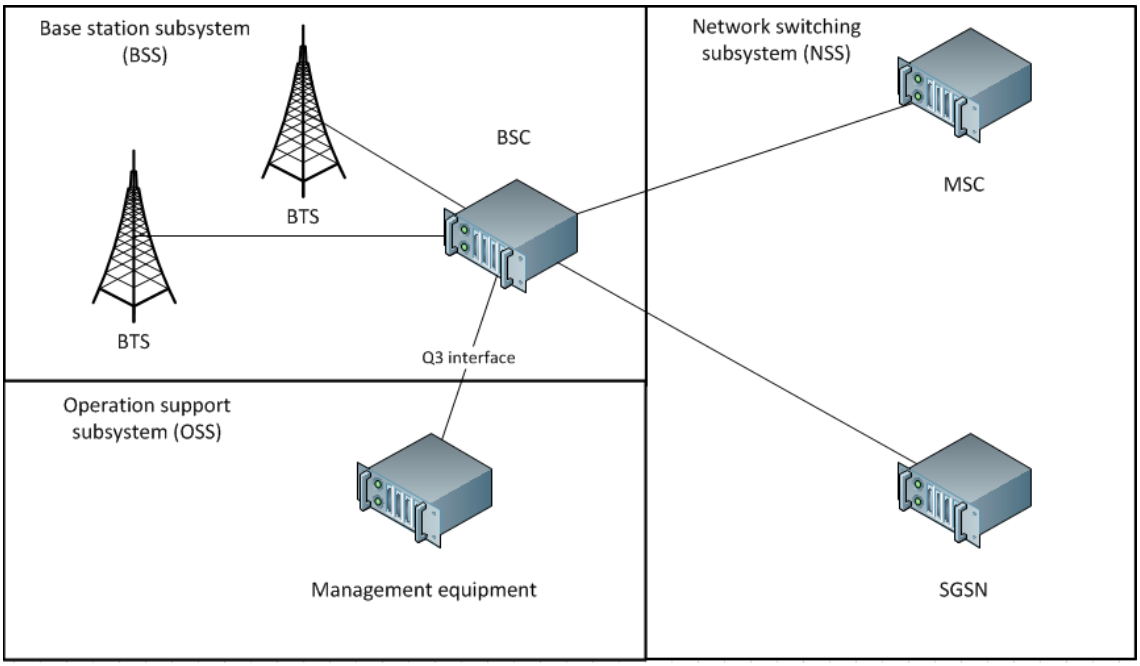

Figure 1. The GSM network can be divided into three segments which the BSC interconnects.

The BSS consists of BTSs (base transceiver station) and BSCs. The BTS establishes and maintains connection to MSs (mobile station) for example a mobile phone within the cell. The BSCs control BTSs with several parameters for example used frequencies and power levels. One BSC can have several BTSs attached to it. In overall the BSS provides ways for the MS to connect to GSM network. (GSM – Global system… 2011, 589.)

The NSS contains MSCs (mobile switching center) and various authentication entities. It provides the MSs ways to communicate with different networks for example land line networks or GPRS (general packet radio service) transmission through SGSN (serving

GPRS support node). Authentication is used for authorizing MSs to connect the GSM network. (GSM – Global system… 2011, 590.)

The OSS collects information about the whole GSM network performance and MSs. The collected information from MSs contains billing information for service providers. The BSS performance information is collected through Q3 interface figured in Figure 1. (GSM – Global system… 2011, 590.)

2.1. Base station controller

"The base station controller provides, classically, the intelligence behind the BTSs. Typically a BSC has tens or even hundreds of BTSs under its control. The BSC handles allocation of radio channels, receives measurements from the mobile phones, and controls handovers from BTS to BTS (except in the case of an inter-BSC handover in which case control is in part the responsibility of the anchor MSC). A key function of the BSC is to act as a concentrator where many different low capacity connections to BTSs (with relatively low utilization) become reduced to a smaller number of connections towards the mobile switching center (MSC) (with a high level of utilization)." (Wikipedia 2012.)

The BSC is undoubtedly the most robust element in the BSS as it is not only a BTS controller but, for some vendors, a full switching center, as well as an SS7 (Signal System no. 7) node with connections to the MSC and SGSN when using GPRS. It also provides all the required data to the OSS as well as to the performance measuring centers. (Wikipedia 2012.)

The databases for all the sites, including information such as carrier frequencies, frequency hopping lists, power reduction levels, receiving levels for cell border calculation, are stored in the BSC. (Wikipedia 2012.)

2.2. Circuit-switched transmission

Traditional transmission of the GSM is CS-based (circuit-switch) end-to-end network where the traffic reserves a dedicated channel (circuit) to transmit various data types for example call data. The channel can't be shared with any other connection which means that the channel bandwidth is guaranteed from the starting point to the ending point.

Minimum bandwidth for CS-based transmission is ANSI (American national standards institute) T1 (1,544kbit/s) in North America and ETSI (European telecommunications standards institute) E1 (2,048kbit/s) in Europe. T1 can serve 24 channels and E1 32 channels concurrently. (Wikipedia 2012.)

TDM (time-division multiplexing) is a technology used in CS-based networks especially in telecommunications. TDM makes possible to transmit several channels in one circuit by creating sub-channels. (Wikipedia 2012.)

2.3. Packet-switched transmission

PS-based (packet-switched) transmission uses smaller data blocks called packets to reach the destination. Whereas CS-based traffic used dedicated channel to transmit data PS-based traffic uses best available route to reach the destination by utilizing different techniques and protocols.

PS-based transmission benefits for GSM network is described later at Network conversion from circuit-switched to packet-based transmission.

For modeling the PS-based transmission different models have been introduced. One of these is based on IETF (Internet engineering task force) RFC (request for comments) 1122 which describes the transmission by dividing the transmission to four different layers as figured at Figure 2. The model provides means to understand how each layer provides methods called protocols to transmit the packet through the network.

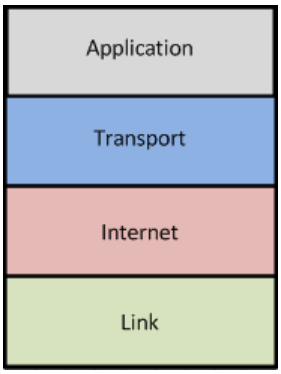

Figure 2. TCP/IP model is divided into four layers which each has its own purpose.

2.3.1 Link layer

The link layer provides protocols to transmit a packet between two hosts within the same network for example from the BSC to the BTS. Popular link layer protocol is IEEE 802.3 Ethernet. IEEE 802.1Q protocol frame in Figure 3 is enhanced version of IEEE 802.3 frame which can be used for dividing the network to multiple VLANs (virtual network) by adding a field to Ethernet packet called frame.

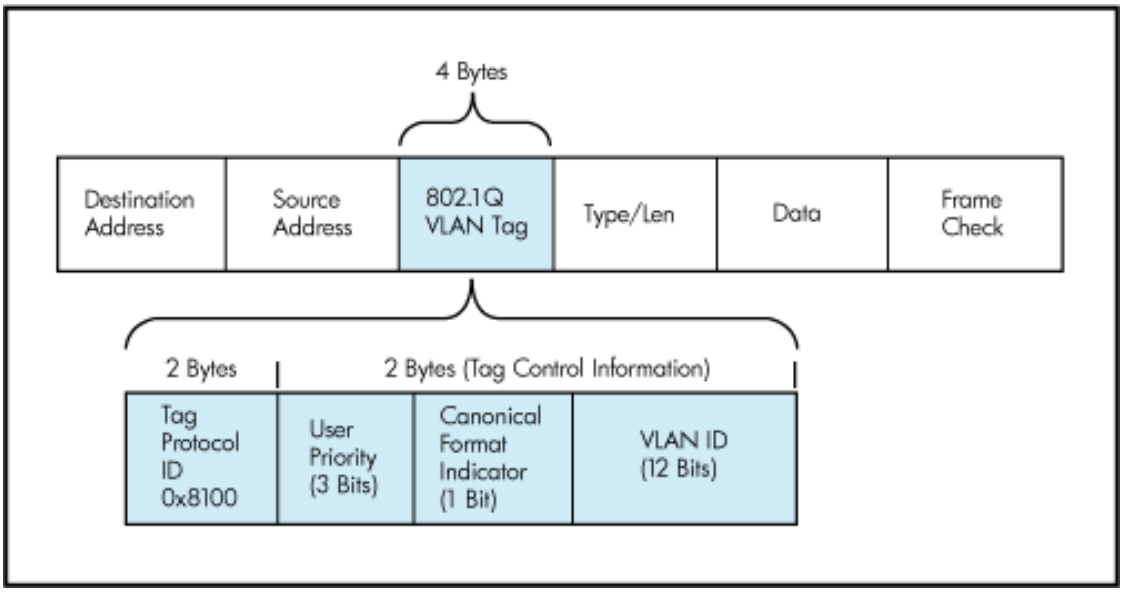

Figure 3. IEEE 802.1Q frame contains information about used VLANs within Ethernet frame. (zanetworker 2011)

Data transmission between hosts is achieved by utilizing the address fields. Frame check is a field which can be used for checking the packet integrity. Data field contains information of the next layer.

There are three different transmission types which can be achieved by different values of the address fields. The networking company Cisco (2006) has defined the transmission types as follows:

- unicast – one host to another
- multicast – one host to multiple hosts
- broadcast – one host to all hosts within the same network

These types make possible to provide various services to network for example efficient distribution of video streams with multicast.

2.3.2 Internet layer

Internet layer provides means to establish connections between two or more different networks (IETF RFC 1122 1989, 27). IP (Internet protocol) is popular Internet layer protocol. There are two versions of IP.

IPv4 (Internet protocol version 4) has been there for more than twenty years. It seems that locally it is preferred for its maintainability and easy deployment. For such old protocol it is researched in many occasions regarding security and although there are many issues they are known. IPv6 (Internet protocol version 6) is new comparing to IPv4 and there hasn't been so much time to research it. It might have some critical flaws regarding the whole protocol design which can be fatal to telecommunications network.

The same transmission types are present in the Internet layer as in the link layer (IETF RFC 1122 1989, 28-29).

The connections between different networks are established by technique called routing. The routing is utilizes source and destination address fields figured in Figure 4 to transmit IP datagram between two networks.

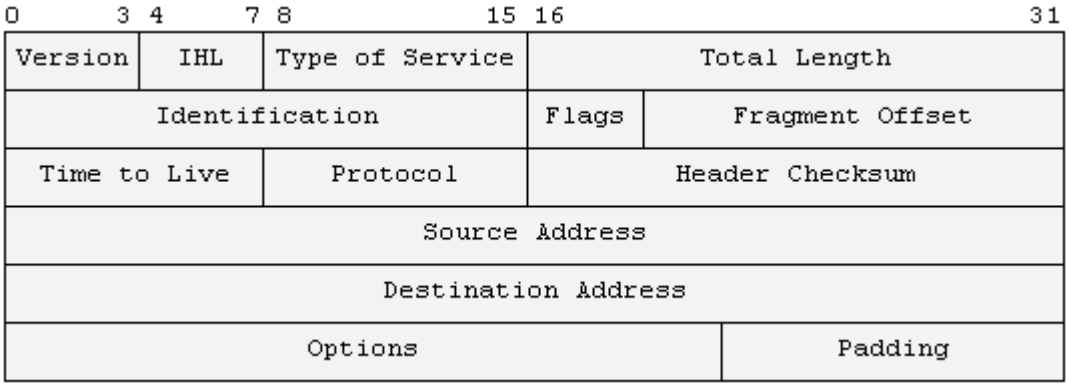

Figure 4. IPv4 datagram header contains fields which are utilized in various Internet techniques. (Freak labs 2007.)

2.3.3 Transport layer

Transport layer handles host-to-host communication. For example TCP (transmission control protocol) can be used for providing reliable connection between hosts by using packet sequence numbers and integrity checks. UDP (user datagram protocol) is more

preferable for telco networks because it provides fast way to transmit packets between hosts. It doesn't implement reliability measures as TCP does. SCTP (stream control transmission protocol) combines reliability from TCP and speed of UDP. SCTP can be used for transporting signaling information and data in the same packet. (IETF RFC 2960 2000.)

Connection between hosts is established between ports. Port is virtual connection point of a host. Port numbers are provided in Transport protocol packet header figured in Figure 5 in a 16 bit fields. Therefore the range of ports is 0 to 65535. Some ports can be registered to a certain application and so it is identifiable more easily.

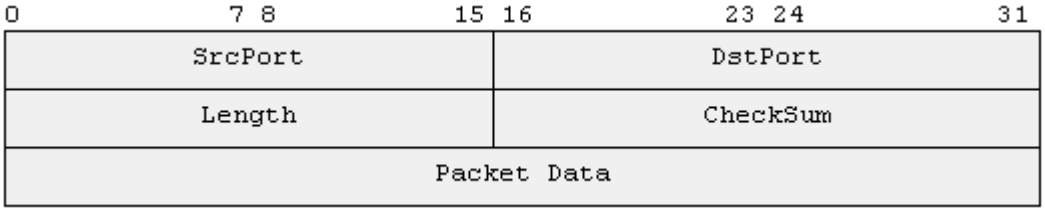

Figure 5. UDP packet contains only necessary information to achieve fast but unreliable transmission. (Freak labs 2007.)

According to IANA – Service Name and Transport Protocol Port Number Registry (2012) the registered ports are described as follows:

- The range from 0 to 1023 is used for well-known services to connect for example file transferring service FTP in TCP port 21 or secure shell connection SSH (secure shell) in TCP port 22.
- The range from 1024 to 49151 is known as registered ports. This range is used for providing a regular port number for requested application. Port is marked as registered after IANA is accepted the request to use this port number for application.
- The range from 49152 to 65535 is free to use. This range can be used in telco networks for example providing voice data connection.

The registered port ranges are only applicable in TCP and UDP protocols. There are various other protocols as well for different sometimes specialized needs. In these the port numbers aren't restricted in any other than the 16 bit field way.

2.3.4 Application layer

Application layer provides services for both network and end users. For example SSH protocol can be used as a secure way to connect to BSC and NTP (network time protocol) provides timing information for clients. Application contains means to achieve synchronization of telco network with Synchronous Ethernet protocol or Precision Time Protocol.

2.4. Network conversion from circuit-switched to packet-based transmission

TDM or generally circuit-switched transmission is slowly moving towards Ethernet and IP or generally packet-based transmission. There are several causes which support the change. What this change means concerning the security?

Due to the nature of packet-based transmission the traffic will be burstier because it doesn't reserve the whole bandwidth anymore as it did with TDM. Due to the possibility of routing the packets of one connection via different routes the reordering of packets must be handled in order to establish a steady connection for telco. Because packet-based transmission techniques are virtually the same all around the world the potential attackers are also all around the world. This raises numerous security threats towards the BSC.

Unified technique infrastructure brings savings by sharing the same media with other radio access technologies like WCDMA (Wideband code division multiple access) or LTE. Savings are achieved by co-siting the different technologies also. Whereas GSM needs reliable connection the latter technologies need high speed availability. By packet-based transmission both reliable and high speed are achieved with smaller costs.

3 SECURITY CONCERNING BSC

Various requirements are demanded by the whole GSM network by different organizations regarding the security. Some of these requirements concern the BSC too. The security can mean both confidentiality and network availability aspects. The availability of the network can be severed by various attacking methods against the devices which do the networking tasks. The confidentiality of a call or data is lost when the interception is made to the call connection.

3.1. General security aspects

3GPP 42.009 (2003, 6) states that GSM network must contain security features to ensure the confidentiality of user data of MSs and validity of used MSs. ”*Security features provided in a GSM PLMN (Public land mobile network)*
The following security features are considered:

- *subscriber identity (IMSI) confidentiality;*
- *subscriber identity (IMSI) authentication;*
- *user data confidentiality on physical connections;*
- *connectionless user data confidentiality;*
- *signalling information element confidentiality.*

The implementation of these five security aspects is mandatory on both the fixed infrastructure side and the MS side.”

The BSC is part of the fixed infrastructure so these aspects apply to BSC too. The BSC must ensure transmission information confidentiality but it is transparent to any authentication methods provided by the MSs.

3.2. Attacking methods

The packet-based transmission techniques are implemented throughout the world. This brings several attacking methods against the BSC too.

3.2.1 Flooding

The objective of flooding is to cause loss of service and incorrect behavior at target systems through resource exhaustion, interference with legitimate transactions, and exploitation of buffer-related software bugs. Flooding may be directed either at the actual host or at resources in the intervening IP Access Links or the Internet. Where the latter entities are the target, flooding will manifest itself as loss of network services, including potentially the breach of any firewalls in place. (IETF RFC 2960 2000, 115.)

"Smurf Attacks - This attack uses IP spoofing and broadcasting to send a ping to a group of hosts on a network. When a host is pinged it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to network, all hosts will answer back to the ping. The result is an overload of network and the target system. The only way to prevent this attack is to prohibit ICMP traffic on the router." (swati 16 2009.)

There is a flooding method figured in Figure 6 which implements spoofed source address in IP datagram header. After the destination host response to this datagram it is routed back to the sender which is in this case every host in the same network.

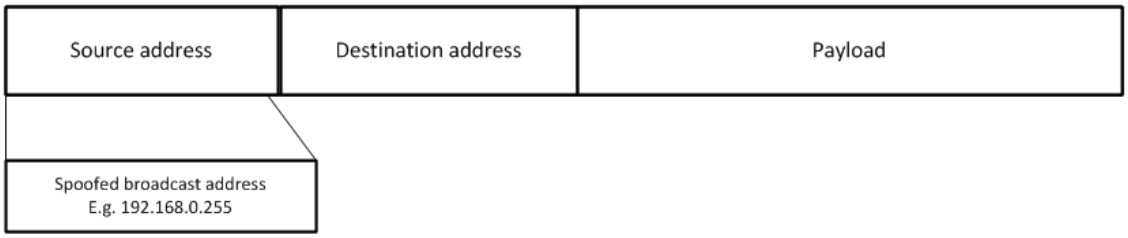

Figure 6. The Internet layer packet header can contain spoofed source address which can cause flooding in the network.

These methods can bring the BSC to denial of service state which prevents any traffic going through the BSC. Depending on the attack interface this could mean the loss of calls or loss of management or both.

3.2.2 Interception

The interception means a state in communications when confidentiality of the connection is lost. The method is used in various data gathering situations or eavesdropping the caller.

The BSC has Q3 interface seen in Figure 1 which is used for management information retrieval. If this interface wasn't secured the information could be intercepted and the attacker could have information about the BSC. After this the information could be used to create an attack against the BSC.

If MS uses GPRS connection to transmit data for example http traffic the packets could be sniffed and some confidential data could be revealed to attacker.

Interception could be used also on call traffic if the traffic isn't secured properly. This would need other devices too but the interception can be made still.

"TCP Sequence Number Attack - This is when the attacker takes control of one end of a TCP session. The goal of this attack is to kick the attacked end of the network for the duration of the session. Only then will the attack be successful. Each time a TCP message is sent the client or the server generates a sequence number. The attacker intercepts and then responds with a sequence number similar to the one used in the original session. This attack can then hijack or disrupt a session. If a valid sequence number is guessed the attacker can place himself between the client and the server. The attacker gains the connection and the data from the legitimate system." (swati16 2009.) The attacker can get caller data which can be used to produce rogue MSs.

3.2.3 Denial of service

Denial-of-service is used for halting the processing of packets in the target machine. Usually the DoS state is achieved by sending malformed packet to target or exhausting the target of resources. There are many levels where vulnerabilities can manifest. Protocol implementation or even specifications can have flaws in them.

”The SYN flooding attack is a denial-of-service method affecting hosts that run TCP server processes. The attack takes advantage of the state retention TCP performs for some time after receiving a SYN segment to a port that has been put into the LISTEN state. The basic idea is to exploit this behavior by causing a host to retain enough state for bogus half-connections that there are no resources left to establish new legitimate connections.” (W. Eddy 2007, 1.)

In some cases there has been DoS state when the host has received zero length packets. Usually the situation has been in applications but it doesn’t mean that the used library stack of the implementation is secure. Most times zero length packets are dropped by firewall or discarded by the host.

Application layer services on operating system can have various vulnerabilities because they can utilize different layers of TCP/IP model. Usual flaw concerns some basic process of an application like authentication. If intentionally malformed value is as input the application stops responding.

FTP (file transfer protocol) shouldn’t be used at all because there is a secured version of ftp, SFTP (secure file transfer protocol). FTP server can have a flaw for example when the input is bigger than certain amount of characters the server doesn’t respond anymore. As mentioned the FTP is used to transfer data between hosts. This function is useful for example when the update for unit has to be moved to the unit. If the server is unavailable the update file cannot be transferred.

HTTP (hypertext transfer protocol) server can be stopped by sending thousands of HTTP Get-messages to the server. This exhausts the server and it stops responding. Secured version of http can be used instead if it’s needed. Although the secured version doesn’t remove the DoS attack it adds an encryption to the traffic between the host and the server. HTTPS (secured hypertext transfer protocol) has also vulnerabilities but there are several workarounds known to these issues. If the Q3 interface is implemented by using http server this attack makes the BSC unavailable for management.

Used operating system can has vulnerabilities which are caused by unsecure programming. These vulnerabilities are often manifested by overflows of some implementation. This overflow then gives attacker a possibility to run his own code. Most famous would

be SQL (simple query language) injection which doesn't work on the BSC because no SQL databases are used.

DoS state can be achieved by sending just so many packets to the interface that its out-bound queue is full and packets are discarded. This can be avoided by using queuing methods.

"The ping of death operates by sending Internet control message protocol (ICMP) packets that are larger than the system can handle. Buffer overflow attacks attempt to put more data into the buffer than it can handle. Code red, slapper and slammer are attacks that took advantage of buffer overflows, sPing is an example of ping of death." (swati16 2009.)

4 PREPARING FOR AN ATTACK

Various preventive and protective measures are developed against the previously presented threats. These don't necessary remove all the possibilities to prevent the whole attack but the attack can be controlled in most known cases. If the attack occurs there are several management options to implement in the network which help to minimize the impact.

4.1. Protection mechanisms

There are several devices and mechanisms which can be used for controlling the attack against the network.

4.1.1 Firewall

Firewalls are used to block unauthorized connections and filter unwanted traffic to the network. Firewalls can be implemented in the upper three layers of TCP/IP model described in Figure 2. Implementation methods can be as follows:

- Internet layer: Filter packets from certain IP address
- Transport layer: Filter traffic from or to certain ports
- Application layer: Filter traffic from or to certain application

(Wikipedia 2012)

Firewalls can be used for interrupting SYN flooding attack by splitting the connection between the attacker and the hosts as figured in Figure 7. When the firewall responds to the TCP-SYN packets no resources are taken on host platform.

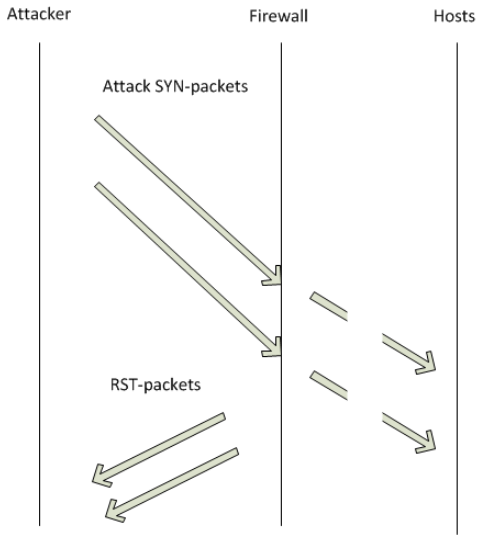

Figure 7. Firewalls can intercept SYN flooding attack by sending TCP RST-packets to reset the TCP connection.

4.1.2 Intrusion detection system

IDS (Intrusion detection system) is used for detecting intrusions into the network. It sniffs the traffic and if known attack fingerprint is detected it raises alarm. The IDS doesn't prevent any attack but it informs the administrator of potential attack and therefore gives time to respond. The intrusions are recognized by fingerprints. When the attack is launched the order of launched procedures matter. How the attack is launched forms the attack fingerprint.

4.1.3 Intrusion prevention system

IPS (Intrusion prevention system) is used for preventing intrusions into the network. Together with IDS it inspects the traffic within and to the network. If an intrusion is detected IPS policies define how the system reacts. It can for example drop all the specified traffic to the network and inform the administrator of breach.

4.1.4 Securing traffic

The connection can be secured by establishing an IPSec tunnel between network entities for example BSC and BTS. There are downsides when using IPSec tunnels because they must be properly configured. If the misconfiguration happens the tunnel is established over and over again and any traffic doesn't get through. The tunnel establishing

process is pretty heavy and it might raise some performance issues by using processor for calculations.

”IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPsec uses two protocols to provide traffic security: Authentication Header (AH) and Encapsulating Security Payload (ESP).

- *The IP Authentication Header (AH) provides connectionless integrity, data origin authentication, and an optional anti-replay service.*
- *The Encapsulating Security Payload (ESP) protocol may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service.*
- *Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols.”* (Kent, S. Atkinson, R. 1998, 6-7.)

Securing the traffic with IPSec tunnels the effects of MITM attack is minimal or nonexistent because encryption takes time depending on the used encryption strength.

4.2. Traffic management

The traffic management is an umbrella term for various mechanisms to manage data flows through the BSC. On congestion situations the overall delay can’t rise. For these situations different kind of quality of service methods can be used. The purpose of this is to ensure that the traffic gets through even if there is congestion. The whole process of traffic management is figured in Figure 8.

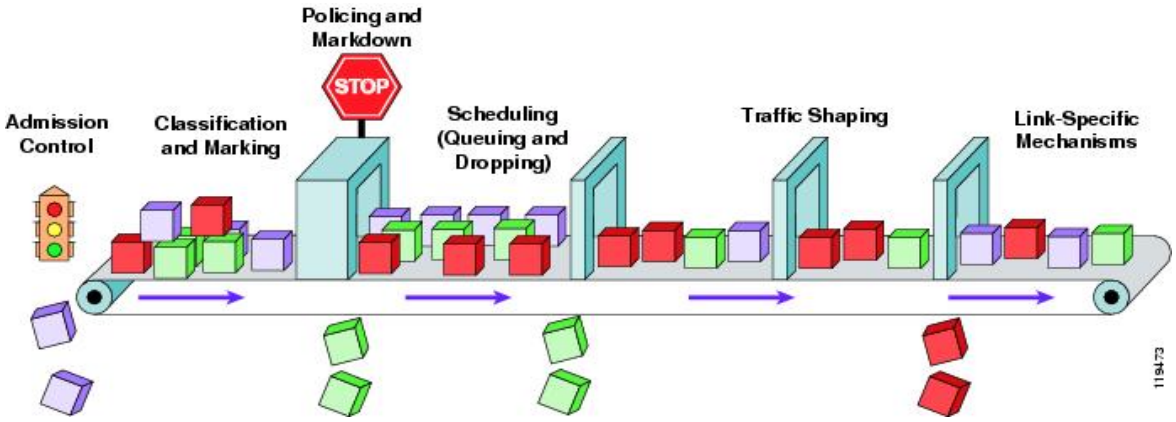

Figure 8. The traffic management consists of different phases. (Cisco.)

4.2.1 Marking

DiffServ is widely implemented marking mechanism. It alters the Internet layer packet by modifying DSCP field in IP datagram header. In theory DiffServ can have 64 different priorities for traffic. (Nichols, K. Blake, S. Baker, F. Black, D. 1998, 6-7 and 13.)

4.2.2 Policing

Policing defines how the marked packets are handled towards the destination. For example a certain traffic flow can be restricted to use only some percent of the available bandwidth. (Cisco.)

4.2.3 Queuing

Queuing methods define on which basis the packet is dropped if the input or output queues are full or nearly full. Two example of queuing methods are defined next:

- *”WFQ (Weighted Fair Queuing) gives low-volume traffic flows preferential treatment and allows higher-volume traffic flows to obtain equity in the remaining amount of queuing capacity. WFQ tries to sort and interleave traffic by flow and then queues the traffic according to the volume of traffic in the flow. Therefore, the fairness in WFQ is that the larger traffic flows (greater in byte quantity) do not arbitrarily starve smaller traffic flows by consuming all the bandwidth.*

- *FIFO (first in first out) is the default mechanism used on routers. It is considered a store and forward method. During congestion periods, packets are stored in a queue, and then forwarded in the order in which they were received when the network is not congested."* (Microsoft support 2007.)

4.2.4 Shaping

Shaping can be used when there are differences between bandwidths on the network. If the edge is only a ANSI T1 or ETSI E1 connection and before that there is 100 megabit connection the bottleneck might occur on the T1 interface because it can't send as fast as its receives packets from the faster connection. By shaping the traffic a constant flow of packets is achieved.

On the shaping phase the shaper chooses packets from the defined queues by utilizing certain mechanisms. After that it sends the chosen packets through the media to the destination.

4.3. Site equipment

Although the focus of the thesis isn't on the site equipment it is still necessary part of telco network. When deploying site equipment basic principles of security apply on those too. Equipment must be physically secured and after that comes the configuration. Port-based security configuration affects physical security also because the equipment isn't accessible from physical location.

Different vendors of devices use almost always their own operating systems on networking devices. Nothing is impenetrable so the more different device platforms there are the more vulnerable interfaces there could be. Therefore it is very important to update operating systems to newest possible version.

5 TESTING PROCESS

Security testing doesn't differ much from any other specific process. It needs resources, proper documentation before, during and after the testing. However software resources contain tools which can be interpreted as hacking tools and therefore illegal in many countries.

Process should be iterative in every release. It is advisable to iterate the process even within the same release for monitoring purposes.

5.1. Resources

Testing process contains many different resources that need planning. This project needed human resources for actual testing and managing the overall process.

The project needs also the hardware resources. There are two kinds of hardware resources: the tested system and the testing equipment. The tested system is a BSC which can be for example FlexiBSC. The capacity of the BSC must be planned too. The amount of planned capacity takes more time both in deployment and in testing because there are more interfaces to be configured and tested.

Another hardware resource is the testing equipment which contains the testing software. The configuration of the testing equipment is needed because the capability matters very much when executing test cases. The speed of processor has straight impact on how much requests it can spawn when doing robustness testing. The specification of used equipment has straight impact of overall experience of the operating system.

Software resources consist of running operating system and testing tools. Chosen operating system limits testing tool range because all available tools aren't supported in every major platform.

Example testing tools are described more in Execution. It takes time to learn to use these programs especially if started from scratch. Concurrent testing can be done with some of the lighter tests for example port scanning. This can be automated with scripts

also so the analysis phase can be done concurrent with the testing. The scripting language depends on used platform for example shell scripting in Unix/Linux-based systems and PowerShell in Windows environments.

5.2. Legal issues

Because the nature of security testing can be compared to hacking in many countries the owning of hardware or software is prohibited. Some countries might have more loose restrictions and prohibit only activities counted as hacking.

In some cases the permission can be obtained from authorities. Company can have an employee who handles the legislative aspects of testing. This employee can allow security testing in laboratory network in most cases too.

Finnish law prohibits later described activity as security breach or intent to harm target system which are punishable by fine or imprisonment. These are described more in detail at Finnish Criminal Code Chapter 38 Section 5 and 8 and Chapter 34 Section 9 ab.

Common method in security testing is port scanning which was litigated on highest level of civil legislation and was punished in the trial. Case can be found only in Finnish. (Markku Fredman, Petteri Järvinen. Tietomurto.)

There can be some nearer and more local restrictions which might apply to testing. Different kind of companies can have policies and guidelines concerning the security aspects. Most of times these policies are based on ISO (international standardization organization) 27000 series certificate guidelines which are as general as they come. Though the policy can has appendices regarding the testing procedures.

5.3. Communication matrix

Communication matrix is summary of all relevant connections of BSC. It contains information for example which ports are used for transmitting call data from BSC to MSC.

Depending on the amount of documented devices the matrix can be small or big. If there are many different platforms the matrix can be done all of them to keep the size small. This brings problems when some form of summary must be presented of connections. Depending on the tool to create the matrix the maintenance of the matrix can be very easy. If the tool has possibility to filter the data according to some column value the maintainability isn't difficult and it can be done in one big table.

In the attached matrix in Appendix 1 all relevant example connections are summarized in one table with the possibility to filter the data with different parameters. Most usable parameters are hardware platform and software revisions named S14 or S15.

Matrix can be used as a measure of quality too. Regular testing is easier to done when available connections are documented properly. In my opinion the matrix should be added to the material delivered to customer by default. This could raise confidence towards the company's quality control.

Matrix should give an explanation to questions what, when, how, where and why in following fashion:

- Hosts are divided in two end points: the local and the remote. The local end point refers to unit or system in the BSC to be tested. The remote end point refers to another BSC or some other element for example the base transceiver station. Local unit and remote system act as hosts in attachment matrix.
- Before the connection is available it must be initialized. One of hosts must have a need to establish a connection. In client-server environments the initializing host is client (←, →). But there are situations when the initializing host can be either one of hosts. This could be marked as both-way initialization (↔).
- Protocols are used for providing ways to communicate between different parts of the network. For example IP Mobility protocol is used to maintain the same IP address when moving between two different cells.
- Ports are virtual connection platform where the connection is possible to establish between hosts. Ports can be used for identifying services and therefore it's important to document which services are enabled on BSC and in what ports.
- Services are applications which need a network connection. Application is the reason why the entry is added to the matrix. For example management application needs a connection and therefore an entry to matrix. Services or connections

are spawned by some feature. This can be basic functionality of the system or customized or value added functionality. For management purposes the spawning feature should be mentioned in the matrix.

If matrix is delivered to testing authorities it is important to add on which platforms and versions the connection is available. S14 and S15 columns in the Appendix 1 provide the version information and Related feature column the feature which presents the connection.

Matrix should contain only relevant services. There can be some debugging properties enabled which aren't needed in customer environments normally.

5.4. Testing metrics

Telco networks are considered as high availability services. They should work under heavy load flawlessly. Therefore there must be some metrics which provide the information about the network health. Because the traffic is packet-based the regular delay and packet-loss are sufficient metrics.

These metrics are applicable only in the call data or data services. The BSC management traffic doesn't have to meet these requirements.

The delay and packet-loss are considered as technical requirements for telco networks. The simulated or real calls are more relevant metrics when doing the testing in high level but technical metrics can be used if more fine-grained testing is done.

5.4.1 Delay

Delay is considered as technical requirement for the whole telco networks. Although there are several different specifications depending on used transport technique for example satellite or optical all of these have some value for the delay requirements.

ITU-T G.114 (05/2003) states that one-way overall delay of IP-based network has to be under 400 milliseconds. Preferable value is under 150 milliseconds which is achieved in local mobile networks. Calculations regarding this requirement differ from circuit

switched traffic in many ways. For IP-based networks there is a possibility to pack many voice frames to one packet whereas on legacy techniques packages are sent in voice frame basis.

5.4.2 Packet-loss

Because the developmental time span is huge in the used voice codecs there has been time to address the packet-loss issue. For this reason the precise number of dropped packets cannot be universal. There are several codecs for voice and some of them are proprietary and some referred as open. During the developmental cycle of codecs there has been also time for considering the packet-loss issue. Most of the codecs can adapt to the loss and the change is unnoticeable to caller. Voice codecs contains different amount of speech data so the quality is the main reason for development. For this reason the codec can sustain different amount of dropped packets. The more speech data the codec can encode usually the fewer dropped packets it can sustain. Principles of calculating packet-loss are defined in ITU-T G.113 and ITU-T G.107. (ITU-T G.113 2007 & ITU-T G.107 2009.)

5.4.3 Call

If the previous requirements aren't met by system the customer sees this as unsuccessful call. The call must stay online if some of these values are changed temporarily over threshold value. If the call stays online that doesn't mean that a new call can be made though. The difference between these actions are that for ongoing call the resources are reserved already whereas the new call needs much of signaling information to initiate the connection.

5.5. Testing plan

Testing plan is meant to guide what to test and how. There are two kinds of testing plans. General testing plan is more like a guideline for the whole testing. Specified testing plan can contain guides on how to actually implement the test case. Both of these have benefits of their own. The attached testing plan in Appendix 2 contains generic characteristics but guides on tool examples.

If there is a need to start the whole new security testing process the general testing plan might be in order first. This might apply also on when the testing is outsourced or there are several different devices to test. Generality gives freedom to do the implementation but in more specified situations this might be too loose. For that the specified plan might fit better. It doesn't have to contain the actual commands how to test something but might give guides on which tools to use. In this case it has to contain some test cases and objectives too.

Testing plan can be done to certain version or to certain hardware variant. These both are important information when the final report is done about the testing.

5.5.1 Objectives

The creation process for testing plan should be started from thinking what the desired outcomes for the whole testing are. The objective is to test if all connections defined in existent communication matrix are as presented and no possibilities for mentioned threats are found present at the tested system.

In the attached testing plan another objective is to verify the availability of BSC in robustness testing.

According to Turpe, S. Fraunhofer Inst. SIT and Eichler, J. (2009, 205) the objectives can be described as follows:
"Objectives of a penetration test vary and have to be agreed upon by the stakeholders of the test. Objectives can be categorized using the following general aims:

- *Identifying vulnerabilities*
- *Improving the security of technical systems as well as of the organizational and personnel infrastructure*
- *Confirming the IT security by an independent third party "*

Testing plan mentions how the system is tested:

- one testing pc is present for one testing target
- several testing pcs are present for one testing target
- one testing pc is present for several testing targets
- several testing pcs are present for several testing targets

This chapter is called Testing strategy in Appendix 2.

5.5.2 Test cases

After defining the objectives the ways to fulfill the objectives are planned. Existing communication matrix can be used for guidance to create test cases.

Test cases can be defined as follows:

- **Protocol scanning** is used to find out which protocols are supported or enabled in the target system. This knowledge can be used for planning an attack. Although the used protocols are fairly old and researched there can be still vulnerabilities.

  Port Scanning is used to find out which ports are open in the target system and which services are running in them; what is visible from outside and inside. The scanning has to be performed from every possible target network to ensure that only the right services are visible. Different services should be visible from different networks (Operations & Maintenance network, user data, signaling et cetera).

  Port scanning results are good way to keep a list of available services and used ports. Because there can be thousands of ports open in live situation the laboratory network is good way to check guidelines for connections.
- **Vulnerability scanning** is a technique that is looking for specific patterns that show the existence of a given vulnerability in the system, i.e., of a vulnerability that has been previously published, described and verified in public. It often uses automated tools to perform scanning and generates a report of found potential vulnerabilities. Due to this nature, such tools can be used to test software components that were widely audited (e.g. popular programs and OS components), but it is neither capable of finding new - unpublished - vulnerabilities on a given system, nor can be used against in-house developed applications that do not have a public list of weaknesses.
- **Robustness testing** is a technique where large amounts of automatically generated, intentionally malformed protocol messages are sent to a target. Any crashes, denial of service condition, degradation of service and all other exceptional behavior are an indication of security related flaws in the implementation.

Robustness testing is good way to test if the target's specification maker has thought congestion situations. As it tries to find unknown vulnerabilities, it is good for self-developed software and rarely used applications as well.

- The purpose of **Denial of Service testing** is to protect the system against known Denial of Service attacks. A DoS attack is an attempt to make a computer resource unavailable to its intended users. An easy way is when the target environment is flooded with so many requests that its resources will be consumed and it is no longer able to provide its service for the real requests. DoS attack does not always have to use flooding – more sophisticated attacks can use only small network bandwidth.

Attached testing plan combines DoS and vulnerability test cases as one because they are tested with the same tool.

5.5.3 Attachments

The results must be reproducible so the testing report which is based on testing plan and is one outcome of this whole process. The report has to have used configuration and testing tool configuration as an attachment. Especially important is to get plugin and software versions of used tools. Plugins are vulnerability scanning files from used tools for example files written in NASL(Nessus attack language) in Nessus and OpenVAS tools.

5.6. Testing tools

The security business is as any other business. There are several choices for different kind of situations. The tool has to be able to do Internet layer testing. Application layer testing tool focuses on higher level vulnerabilities.

5.6.1 Commercial tools

Metasploit is exploitation software by Rapid7. It consists of a framework, server software and modules. Framework software itself is free but there are different variants of the actual server software. Modules are very extensive and new exploits are released regularly. Enterprise edition has pretty high price tag $15000 per user per year and cheaper Express edition for $3000 per year per user.

Nessus is very known vulnerability scanning software which contains port scanner abilities too. Vulnerabilities are written in NASL. This makes fast release of vulnerabilities possible. Nessus is easy to use. Pricing is pretty low compared to Metasploit, only $1200 per host.

QualysGuard is popular vulnerability management product. It has easy web-based GUI and contains fair amount of different scanning mechanisms. It has vulnerability support for several operating systems like numerous linux distributions.

Codenomicon Defensics focuses on network robustness testing. Defensics software is very light at first but when it is running it takes resources heavily. It is also easy to deploy and use. Tests can be divided into test suites. Tool has wide variety of protocols to tests especially regarding the telco.

5.6.2 Open source & Free tools

Metasploit community edition has the same framework as the commercial edition but lacks reporting capabilities.

OpenVAS is open source edition of commercial Nessus tool. It has same attack language as Nessus so the same scripts are applicable also on OpenVAS. The tool has regular updates to vulnerabilities.

NMAP is popular port and protocol scanner which is completely free. The basic training material is available free also on nmap.org. The whole training book is available via Amazon.

(SecTools.org)

5.7. Customer environments

During the scanning tool deployment process the deployment of BSC can be started also. Because the BSC deployment process is divided on many different levels the process takes the most time in the whole process.

For reproducible reasons the BSC must be deployed as it is in the customer premises. Because the results of testing can be think as a measurement of quality the results must be based on how the BSC is configured in the customer premises. This can't be the case in every security testing release because the wide variety of customer needs and configurations but it can be think as a guideline for testing configuration.

Benefits of doing like the customers are the results can be repeated in the customer environment in many cases. This can be described as a sense of quality also. Another interested actor in the whole deployment process can be a government.

5.8. Test suites for tools

Testing plan defined in high level what are to be tested in test cases. With the help of these test cases it's easy to create test suites into the tools. Communication matrix can be used as help too when planning protocol or port scanning. The protocol listing from the communication matrix can be used to choose protocol suites in robustness testing tool.

If the testing pc isn't connected straight to the BSC it is very useful to get familiar with the transmission network. Useful information can be bandwidth and site equipment usage or load. This might force to optimize delays and rates in scanning. Because port scans are using raw-IP packets the operating system must be able to form raw-IP packets. This needs root/sudo privileges in Unix/Linux machines and administrator privileges in Windows based operating systems.

5.9. Execution

Before any tests can run the network administrators has to be notified because the tests can have impact on overall network performance. Colleagues have to be notified also because they might be testing on the same network.

Before the first test run the testing equipment must be isolated or walled somehow. There has to be some certainty that any of the vulnerability scan probes aren't found on production network or even in testing laboratory network. If the devices are improperly

configured for example a broadcast storm might happen. Though the network devices would be correctly configured it is good practice to back up the configuration.

According to Turpe, S. et cetera (2009, 206) the risks are described as follows:
”Principal risk factors are the security testing itself, the system under test (test target), the embedding of the test target in its environment, and the operational data residing on the target. In most testing situations one would mitigate the latter three by setting up a dedicated test system in a lab environment using test data, rendering the risk caused by the testing itself acceptable. This is obviously not possible when a production system is to be tested. Security testing causes risks to the target by its very nature. Like an attacker the penetration tester deliberately leaves the relatively safe grounds of intended use and expected activity. Security testing is inherently invasive where it employs techniques similar to those used in an attack. Consider code injection for example, where one attempts to manipulate a system into executing arbitrary code provided by an unauthorized party.”

The testing equipment should be placed in the nearest point possible. This reduces harm and load on site equipment. Because the tested device is both physically and logically one device the optimal point is to connect the testing pc straight to switch port in the BSC.

5.9.1 Protocol and port scanning with NMAP

Protocol and port scanning test cases can be run by NMAP because it has support for SCTP protocol. The following example script in Figure 9 contains functions to run protocol identification scan and TCP protocol port scanning. The same function can be used for UDP and SCTP with small modification done to parameters, -sU for UDP and –sZ for SCTP.

```
function protoscan {
  local TESTCASE=protocolscan
    sudo nmap -sO -vvv -n -Pn --reason --scan-delay 100ms --max-retries 50 \
    --host-timeout 10m \
    -oA $LOGDIR/$DEVICE/$DATENOW.$DEVICE.$RELEASE.$DEVICENAME.$TESTCASE.$SUBNET \
    $NETWORK$IF1,$IF2,$IF3,$IF4,$IF5,$IF6,$IF7,$IF8
}
function tcpportscan
{
  local TESTCASE=portsweep
  local PROTOCOL=tcp
  sudo nmap -sS -O -sV -r -p1-65535 -vvv -n -Pn --reason --max-retries 50 \
  -oA $LOGDIR/$DEVICE/$DATENOW.$DEVICE.$RELEASE.$DEVICENAME.$TESTCASE.$PROTOCOL.$SUBNET \
  $NETWORK$IF1,$IF2,$IF3,$IF4,$IF5,$IF6,$IF7,$IF8
}
```

Figure 9. Protocol and port scanning phases can be executed in their own function in order to get results for analyzing phase.

Used parameters in Figure 9:

- -sO is protocol scanning parameter
- -vvv is verbosity level
- -oA parameter means that result output is put to file. For manageability reason it has long but descriptive file name.
- -n parameter means that no name resolving is done
- -Pn parameter means that application treats every host as online
- --reason gives reason which message is a result of scan for example proto-response if protocol answers to probes
- --scan-delay 100ms is used because testing is done in daytime and there is also other traffic. Every scanning probe which is sent from nmap delays itself 100ms related to other probes.
- --max-retries 50 means that maximum of 50 probes are sent and then the host is marked as unavailable
- --host-timeout 10m means that if the host doesn't answer to probes in 10minutes it is marked as unavailable
- -sS means TCP syn-state scan where syn bit in TCP header is enabled. This way the tcp probes are penetrated through possible firewalls in most cases.
- -O tries to identify the running operating system.
- -sV tries to identify the running service in TCP port.
- -r defines ports to be scanned consecutively
- -p defines the port range

(Gordon "Fyodor" Lyon 2005.)

Different port or protocol states as described by Gordon “Fyodor” Lyon (2009, 77-78):

”Open - An application is actively accepting TCP connections or UDP packets on this port.

Closed – A closed port is accessible (it receives and responds to Nmap probe packets). but there is no application listening on it.

filtered – Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router ruler, or host-based firewall software.

unfiltered – the unfiltered state means that a port is accessible but Nmap is unable to determine whether it is open or closed

open|filtered – Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited.

closed|filtered – This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan…”.

By running the Figure 9 script file the output is presented in Figure 10. NMAP prints only open ports and omits the closed port output to a summary.

```
PORT      STATE SERVICE     REASON  VERSION
22/tcp    open  ssh         syn-ack OpenSSH 5.6 (protocol 2.0)
25/tcp    open  smtp        syn-ack Sendmail 8.14.5/8.14.5
111/tcp   open  rpcbind     syn-ack 2-4 (rpc #100000)
9390/tcp  open  ssl/openvas syn-ack OpenVAS server
44591/tcp open  status      syn-ack 1 (rpc #100024)


TCP/IP fingerprint:
OS:SCAN(V=5.50%D=4/11%OT=22%CT=1%CU=37609%PV=N%DS=0%DC=L%G=Y%TM=4F85EFF1%P=
OS:i386-redhat-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(O
OS:1=M400CST11NW4%O2=M400CST11NW4%O3=M400CNNT11NW4%O4=M400CST11NW4%O5=M400C
OS:ST11NW4%O6=M400CST11)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000
OS:)ECN(R=Y%DF=Y%T=40%W=8018%O=M400CNNSNW4%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=8000%S=O%A=S+%F=AS%O=M400CST11N
OS:W4%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%
OS:W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS:)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%
OS:UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Figure 10. The output contains information of open tcp ports and OS fingerprint if it isn’t identified.

5.9.2 Vulnerability testing with OpenVAS

OpenVAS version 4 is used because it is available in Fedora 15 repositories as of now.

For OpenVAS 4 to work user is to be created with openvas-adduser. Scanning service called openvassd can be started in privileged mode after the user creation. After this the service starts in TCP port 9390 by default and loads available plugins from plugins directory. Plugin repository in OpenVAS website is updated regularly so the update for plugins is available with openvas-nvt-sync in privileged mode.

After this the client software is able to connect to the OpenVAS server. Client connection is shown in Figure 11.

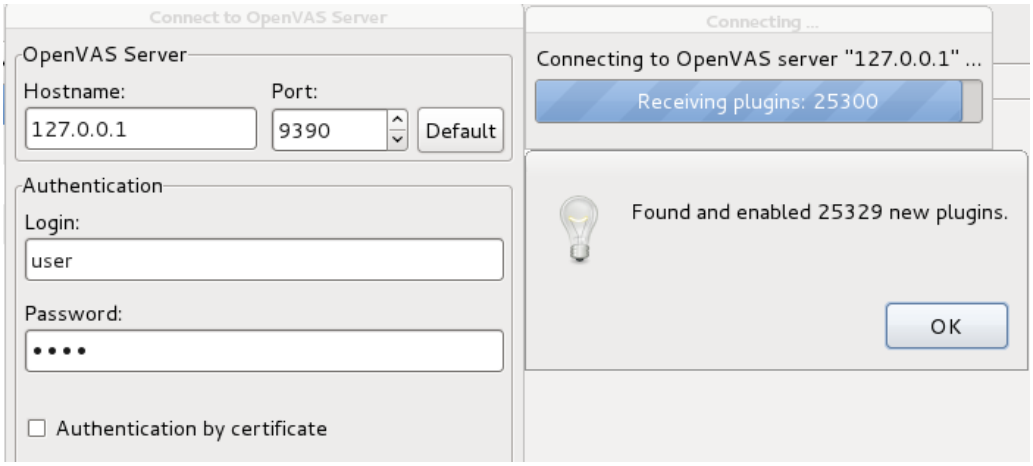

Figure 11. The OpenVAS client connects to OpenVAS scanning service and loads plugins from the server.

After the successful connection to the scanning service the basic view is presented to the user as in Figure 12.

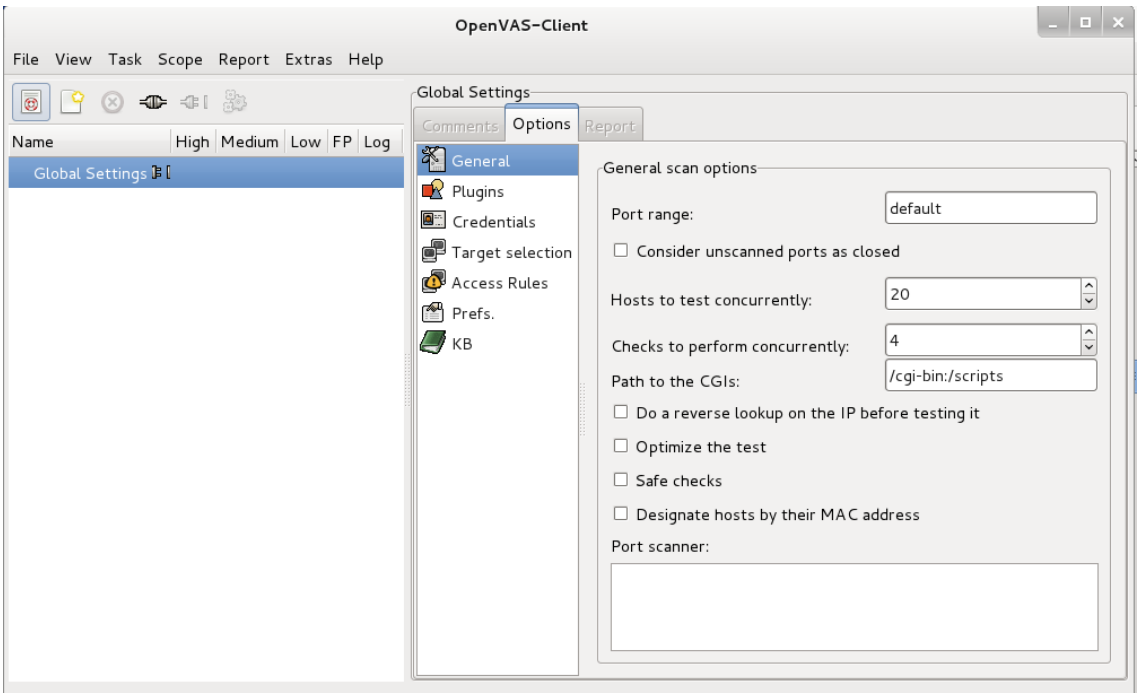

Figure 12. The client shows various options for plugins and scanning service.

OpenVAS is very handy when it comes to manageability. There is a possibility to create so called Tasks and Scopes.

”Tasks are intended to cover all activities of a major topic. A task could be Test the machines of our headquarter or Customer XYZ Inc.

A task can contain a comment that explains the task in more detail. Also any type of additional info or reminder can be entered in the comment area, e.g. when to run the next series of scans or based on which contract the scans are performed.

A task has neither options nor a report. Apart from the comment, it just contains a number of scopes.

A scope can be seen as a sub-task. It defines a certain security scan. The title should indicate the scope of this scan, e.g. Careful scan of web server production system, Aggressive scan of web server alpha test system or All Sun workstations.

Comments can also be specified for each scope and may explain the scope in more detail as well as contain any other helpful hints regarding the respective scope.

Next, a scope may contain a number of reports. Whenever a scope is successfully executed, the resulting report is added to its list of reports.” (Jan-Oliver Wagner, Michael Wiegand, Tim Brown, Carsten Koch Mauthe, OpenVAS Compendium… 2009, 31-32)

Task is named to BSC in Figure 13 because it is the scan target. Scopes are named OS Vulnerabilities to test operating system or platform vulnerabilities and Protocol vulnerabilities to tests vulnerabilities in protocol implementation. This makes it easier to manage the reports which the tool produces after the testing. It is also faster to analyze the results because scopes is done one at a time and therefore produces one report at a time.

Available plugins are shown at Plugins. These can be enabled one at a time or in greater groups.

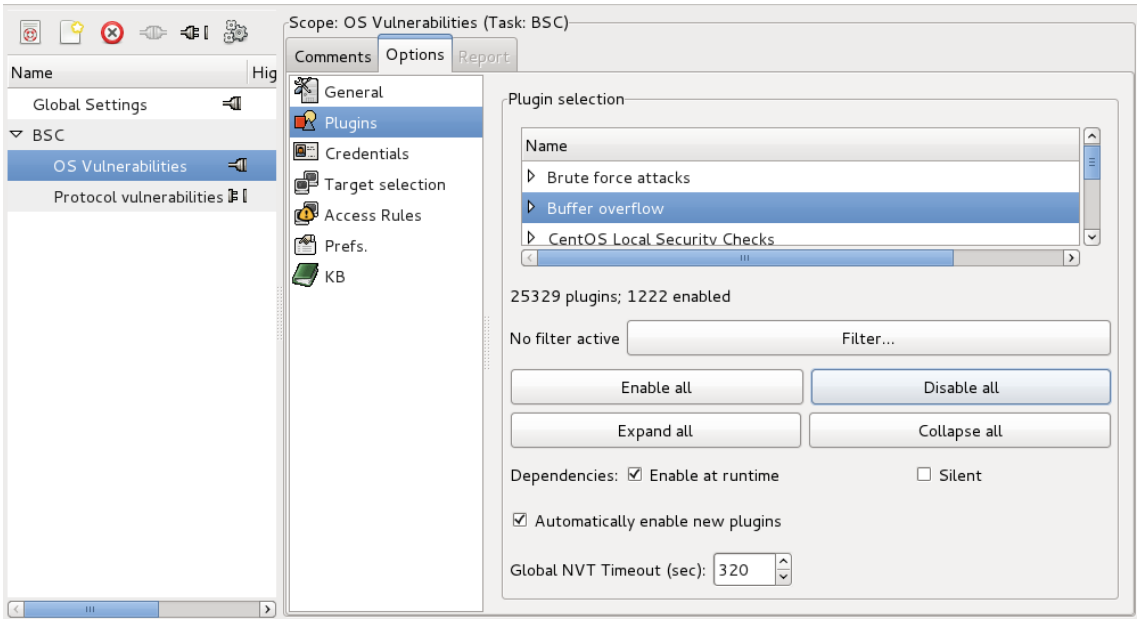

Figure 13. Loaded plugins are divided into various groups by target operating system or attacking methods for example.

Targets can be defined in options tab and target selection as in Figure 14.

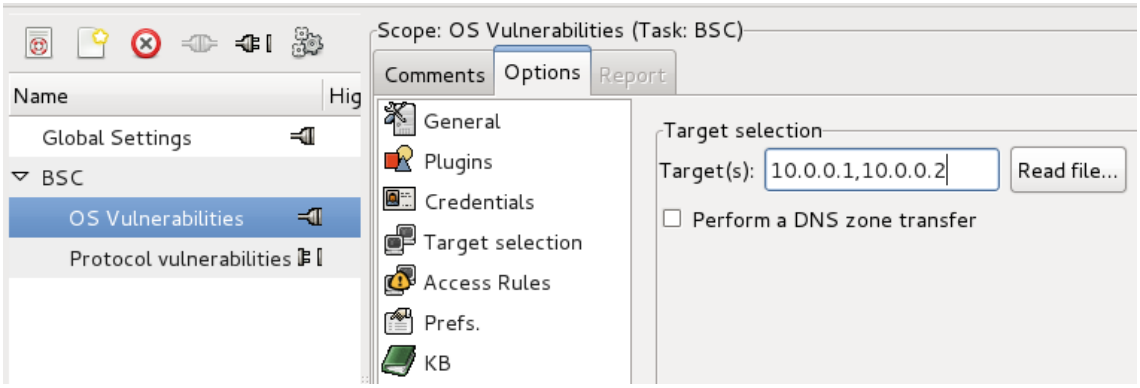

Figure 14. The scanning server can scan multiple targets at once.

The amount of targets and enabled plugins add the testing time. After the testing is completed the report can be reviewed under the Scope as in Figure 15.

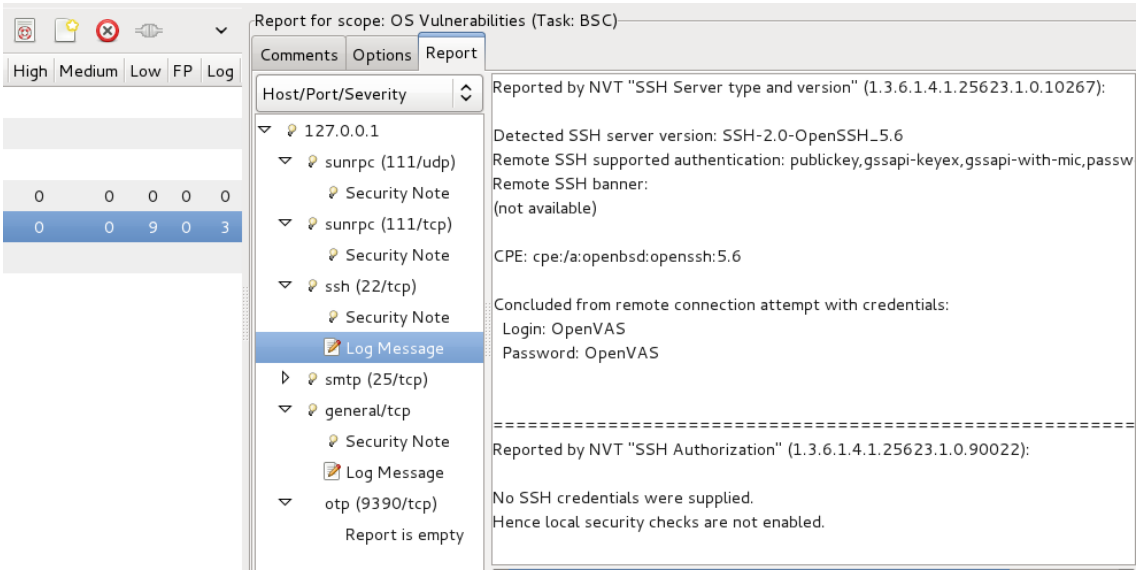

Figure 15. The scanning service shows summarized results after the completion and information regarding the findings.

High level vulnerabilities are marked with red color and shown in high level findings column under the Scope. The information about high level findings is significantly higher comparing to log messages as can be seen between Figure 15 and Figure 16.

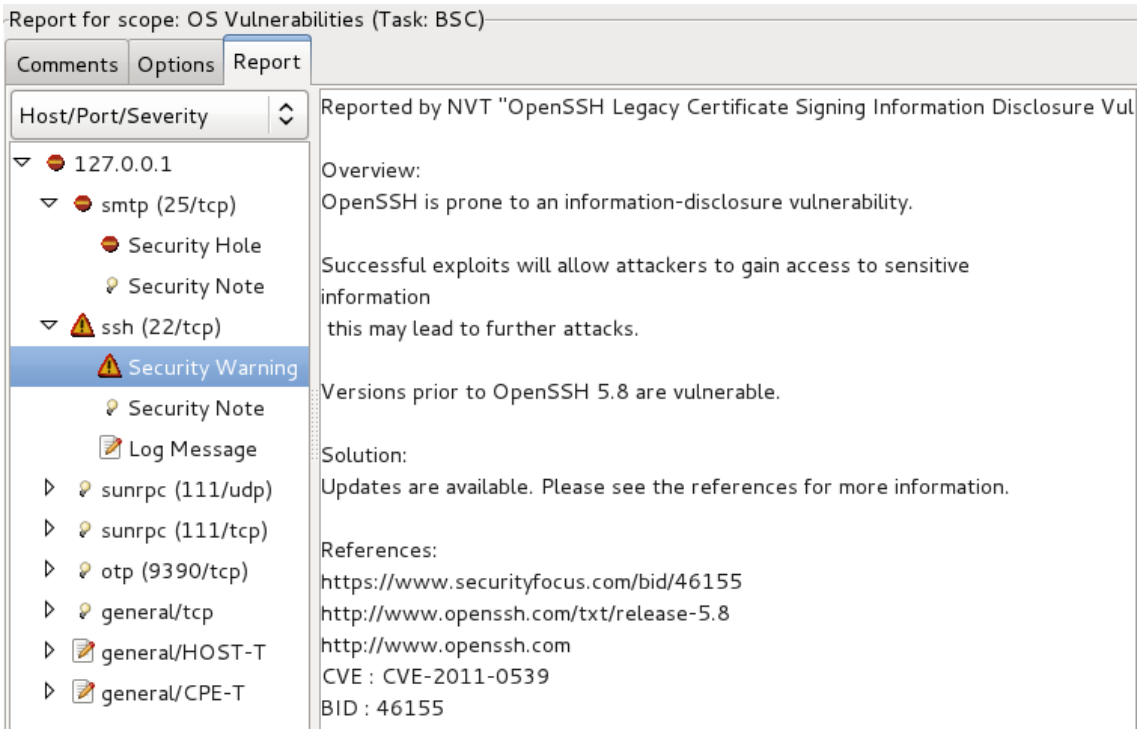

Figure 16. Depending on the severity level the shown messages differ greatly.

Reports can be exported to PDF (portable data format) for example to store it as documentation.

5.10. Findings analysis

The testing tools provide reports which contain the found issues about the testing. These findings have to be analyzed with caution. There are so called false positives which manifests sometimes due to similarities between implemented techniques.

5.10.1 False positive removal

The reports produced by various tools can contain high amount of findings which need to be analyzed. These findings can contain false positives which need to be removed from the final reports because they don't exist actually in the BSC. False positive findings can be for example unsupported protocols listed open in protocol scan reports.

"When exploring a network for security auditing or inventory/administration, you usually want to know more than the bare IP addresses of identified machines. Your reaction to discovering a printer may be very different than to finding a router, wireless access point, telephone PBX, game console, Windows desktop, or Unix server. Finer grained detection (such as distinguishing Mac OS X 10.4 from 10.3) is useful for determining vulnerability to specific flaws and for tailoring effective exploits for those vulnerabilities.

In part due to its value to attackers, many systems are tight-lipped about their exact nature and operating system configuration. Fortunately, Nmap includes a huge database of heuristics for identifying thousands of different systems based on how they respond to a selection of TCP/IP probes. Another system (part of version detection) interrogates open TCP or UDP ports to determine device type and OS details. Results of these two systems are reported independently so that you can identify combinations such as a Checkpoint firewall forwarding port 80 to a Windows IIS server." (Gordon "Fyodor" Lyon , Chapter 8. Remote... 2009.)

Although the database is very good regarding identification process the nature of telecommunications devices make things difficult. Because the devices are highly customized for this special use the identification result is inaccurate most times. In some tools after the unknown operating system has been scanned the tool makes a prediction about

running operating system. The port scanner tool Nmap does this by default. These predictions could vary very much between scanning routines.

Operating system fingerprint can be seen in Figure 10.

5.10.2 Comparison to communication matrix

During the analysis it is good to verify if there were some new ports or protocols open in the results and add them to the Communication matrix if they are relevant.

5.11. Problem mitigation

Even if the newest version of the product is tested there might be some unknown vulnerabilities lying or zero-day vulnerabilities. They are vulnerabilities that don't have any corrections or workarounds yet.

There has to be some person or system which delivers the found vulnerabilities to correct team. If problem correction is done by a separate group the group must be informed and a Pronto raised.

Depending on the used scanning techniques the response for observed problem might change. If penetration testing is used rapid workaround or mitigation plan must be created as soon as possible. Severity level rises as the release is ready to be deployed.

5.12. Testing material sharing

All the produced documentation should be shared to different interest groups. Documentation should be stored to Sharenet where it's widely available to these groups.

Communication matrix should be stored also in the NED tool because it is useful to the customers on planning their own transmission network.

The reports and different result files are recommended to store also on Sharenet. Proper location is in FlexiBSC and BSC3i reserved product areas subfolder Security.

5.13. Testing schedule

Security testing should be mentioned as necessary part of the process in P3 phase where the BSC Program plan is confirmed. By this way the security testing will be done in every release iteratively. Active resources should be allocated to testing in later phases.

Actual security testing can be done in P6 phase where the product is tested in other ways too. There is a possibility to respond to vulnerabilities or other malfunctions yet because the development is in progress. After the working package is delivered for other testing the security testing should start too. One iteration of testing is sufficient to address problems in the beginning. Another iteration should be done in the end of the phase to view if the problems are corrected.

Preliminary reports of testing can be delivered to chosen pilot customers in P7 where the pilots are planned.

All reports and communication matrix should be provided to the customers in P8 when the release is ready for delivery.

6 CONCLUSION

The education material is simple but it gives information about security concerning the BSC. The compact package of different technologies is presented so the personnel can search more information from the references or elsewhere in order to hone the skills. The material isn't supposed to be any kind of final version because the nature of software development is never perfect.

Although described preventive and counter measures are focused on site equipment the same guidelines can be used in the BSC. The BSC has switching units which implements same functions as does the site equipment so the techniques are compatible.

Thesis contains both means to plan and to execute the security testing to the BSC. The most phases are described with examples concerning the BSC. Some factors are pointed out which may have an effect when executing the tests.

6.1. Process time estimates

Time estimates are based on the testing process done to the base station controller. The testing guidelines were based on the process description and the attached testing plan. Presented times aren't absolute but relatively rough estimates.

Planning and deployment: 3 weeks.
The deployment phase consists of:

- choosing the testing tools
- permission request to test
- the BSC deployment
- testing equipment deployment
- testing plan specification
- communication matrix creation

Execution: 1 week.
If one second scanning delay for UDP port is utilized the full scan of 65535 ports the overall time consumption is over 18 hours per host. The hosts can be scanned concur-

rently so the port scans take up to three days depending on the amount of scanned hosts. Vulnerability scan is fast with OpenVAS because it uses only relevant plugins to scanning target. The tests can be done in one day.

Robustness scanning needs the lasting four days because there has to be some additional time reserved if the network or host fails and it must be reconfigured.

Analysis: 1+ week.
Depending on the scope of the testing the needed time for analyses differ from one to two weeks. Analyses for different test cases can be done concurrently with the testing if the test case reports are produced after the test case completion.

During and after the analyses re-runs of the test cases might be in order to verify committed corrections.

Overall: 6+ weeks.

6.2. Testing equipment configuration

The configuration of testing pc can reduce testing time if it has sufficient resources to use. The speed of the processor has impact on how many requests the robustness tool can spawn. The RAM (random access memory) affects the overall performance of the testing pc.

6.3. Quality measurement

The produced documentation from the testing process can be used as measure of quality when presenting the device to customers.

6.4. Development ideas

Because the process model isn’t based on any official certificate it is recommended that for the future the whole security testing process should follow Open Source Security Testing Method. It is more than compatible with the current process. It has very useful chapters regarding the telecommunications network for example Chapter 10. Telecom-

munications security testing. Though it contains unnecessary phases regarding the BSC it can be used as guideline. Chapters 1 through 4 contains basic knowledge about security testing which could give some insight for testing process.

Open Source Security Testing Method can be found at http://www.isecom.org/mirror/OSSTMM.3.pdf.

Some considerations to the traffic management solutions may be found from the MPLS VPN VRF techonology where the whole network is restricted and the traffic can be policed inside the VRF.

REFERENCES

3GPP 2006. TS 42.009 V4.1.0 – 3 Security features provided in a GSM PLMN. Read 4.3.2012. http://www.3gpp.org/ftp/Specs/html-info/42009.htm

Cisco. Quality of Service Design Overview. Read 2.5.2012. http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSIntro.html

Cisco 2006. Inter-Switch Link and IEEE 802.1Q Frame Format. Read 20.4.2012. http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a00800946 65.shtml

Freak labs 2007. Packet sniffing using raw sockets. Read 20.4.2012. http://security-freak.net/raw-sockets/raw-sockets.html

Gordon “Fyodor” Lyon. 2005. NMAP manual page. Read 20.4.2012. http://linux.die.net/man/1/nmap

Gordon “Fyodor” Lyon. 2009. NMAP network scanning web-version – Chapter 8. Read 23.12.2011. http://nmap.org/book/osdetect.html

Gordon “Fyodor” Lyon. 2009. NMAP network scanning.

IANA. 2012. Service Name and Transport Protocol Port Number Registry. Read 1.1.2012. http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

IETF Network working group 2000. RFC 2960 – Stream control transmission protocol. Read 20.4.2012. http://www.ietf.org/rfc/rfc2960.txt

Internet Engineering Task Force 1989. RFC 1122 - Requirements for Internet Hosts -- Communication Layers. Read 20.3.2012. http://tools.ietf.org/html/rfc1122

ITU-T. 05/2003. Record G.114 One-way transmission time. Read 22.2.2012. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.114-200305-I!!PDF-E&type=items

ITU-T. 2007. Transmission impairment due to speech processing. Read 22.12.2012. http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.113-200711-I!!PDF-E&type=items

ITU-T. 2009. Rec. G.107 The E-model: a computational model… Read 22.12.2012. http://www.itu.int/rec/T-REC-G.107-200904-S/en

Jan-Oliver Wagner, Michael Wiegand, Tim Brown, Carsten Koch Mauthe. 2009. OpenVAS Compendium… Read 23.12.2011. http://wald.intevation.org/frs/download.php/558/openvas-compendium-1.0.1.pdf

Kent, S., Atkinson, R. 1998. IETF RFC 2401 - Security Architecture for the Internet Protocol. Read 20.4.2012. http://www.ietf.org/rfc/rfc2401.txt

Markku Fredman, Petteri Järvinen. Tietomurto – oikeustapauskommentti. Luettu 23.2.2012. http://www.fredman-mansson.fi/fi/henkilosto/markku-fredman/kirjoituksia/88-tietomurto

Microsoft support 2007. QoS Queuing techniques. Read 20.4.2012. http://support.microsoft.com/kb/233039

Molisch, Andreas F. 2011. Wireless Communications. 2nd edition. Wiley publishing.

Nichols, K. Blake, S. Baker, F. Black, D. 1998. IETF RFC 2474 – Definition of the Differentiated services field (DS field) in the IPv4 and IPv6 header. Read 20.4.2012. http://www.ietf.org/rfc/rfc2474.txt

SecTools.org Vulnerability exploitation tools. Read 20.4.2012. http://sectools.org/tag/vuln-scanners/

SecTools.org. Vulnerability scanners. Read 20.4.2012. http://sectools.org/tag/vuln-scanners/

Swati16. 2009. Types of attacks. Read 1.2.2012. http://www.unp.me/f140/types-of-attacks-63305/

Turpe, S.; Eichler, J. 2009. Testing production systems safely: Common precautions in penetration testing – B. Objectives. Read 23.2.2012. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5381625

W. Eddy, IETF. 2007. TCP SYN Flooding Attacks and Common Mitigations. Read 3.3.2012. http://tools.ietf.org/html/rfc4987

Wikipedia 2012. Base station controller. Read 23.11.2011. http://en.wikipedia.org/wiki/Base_station_subsystem#Base_station_controller

Wikipedia 2012. Circuit switching. Read 20.4.2012. http://en.wikipedia.org/wiki/Circuit_switching

Wikipedia 2012. Time division multiplexing. Read 20.4.2012. http://en.wikipedia.org/wiki/Time-division_multiplexing

Wikipedia. 2012. Firewall types. Read 20.4.2012. http://en.wikipedia.org/wiki/Firewall_(computing)#Types

zanetworker 2011. Anatomy of a MAC address, BPDU, BID, and the 802.1q Ethernet frame Tag !! Read 20.4.2012. http://adelzalok.wordpress.com/2011/09/29/anatomy-of-a-mac-address-bpdu-bid-and-the-802-1q-ethernet-frame-tag/

APPENDICES

Appendix 1. Communication matrix

Local unit	Local port	Init Direction	Direction	Remote system	Remote port	Protocol	Service name / description	Remarks	S14	S15	HW Platform	Related feature
PCU	N/A	↔	↔	SGSN	N/A	Mobile	Mobility IP	Allows packet data connections in mobile networks to work correctly.				Platform's basic feature
PCU	N/A	↔	↔	Any	N/A	PIM	Protocol independent multicast	Multicast protocol is supported but not used in any unit.				Platform's basic feature
PCU	N/A	↔	↔	Any	N/A	AH	Authentication header	IPSec implementation. Shown when IPSec is enabled. Supported on PCU.				Platform's basic feature
PCU	N/A	↔	↔	Any	N/A	ESP	IKE / IPsec Key Management	IPSec implementation. Shown when IPSec is enabled. Supported on PCU.				Platform's basic feature
OMU	22	←	↔	Management PC	Any	TCP	Secure shell server	SSH is used for securing management traffic				BSSxxxxxx

Testing plan

BSC <Date>

OBJECTIVE

The aim is to verify that only necessary ports are open and protocols are enabled. After the verification process the stability is verified by running robustness test. Testing is focused only on BSC system.

TESTING STRATEGY

Test is conducted from external testing pc to several external BSC interfaces. Connect testing pc as near as possible to BSC to minimize packet drops due to flow control or some other restrictive measures e.g. packet filtering.

Port scanning tool

Use port scanner with UDP, TCP, SCTP support e.g. nmap.

Protocol scanning tool

Use protocol scanning tool to scan which protocols are enabled in the unit e.g. nmap.

Vulnerability testing tool

Use widely available and platform relevant scanning tool e.g. OpenVAS.

Robustness testing tool

If you’re an NSN employee you have access to licensed tool Codenomicon. This is very good tool for this kind of testing.

Hardening

List used hardening measures done to BSC system. Refer to Customer Site documentation.

TESTED PRODUCT

<HW variant><Software revision e.g. RG20>

Number of external interfaces	
Interface	IP address

IPv6 must be disabled and it must be indicated that it is disabled.

Hardening

What measures of hardening is done to product? Refer to Customer Site documentation.

Test case 1 <Protocol scanning>

Used testing tool configuration, see Appendix A

Used device configuration, see Appendix B

Refer to Protocol scanning tool for used tools.

Verification

Open protocols are the same as defined in <communication matrix>.

Results, see Impact analyses

Test case 2 <Port scanning>

Used testing tool configuration, see Appendix A

Used device configuration, see Appendix B

Refer to Port scanning tool for used tool.

Verification

No services are affected by port scans so BSC is available for configuration during port scans. Also one call must be made successfully.

Open ports are the same as defined in <communication matrix>.

If open ports are shown as open|filtered in nmap tool this means that you have to verify if the probes were dropped. Nmap couldn't recognize if the port is open or filtered by any switching units. Usually this means that the port is unreachable from outside.

Results, see Impact analyses

Test case 3 <Vulnerability scanning>

Used testing tool configuration, see Appendix A
Used device configuration, see Appendix B

Verify that all available, relevant and runnable plugins are enabled.

Verification
No services are affected by the vulnerability scans so BSC is available for configuration and monitoring during scan. Also one call must be made successfully.
If serious vulnerabilities are found you must notify responsible person found at Problem mitigation plan.

Remove false positives from results.

Results, see Impact analyses

Test case 4 <Robustness testing>

Used testing tool configuration, see Appendix A

Used device configuration, see Appendix B

Check <communication matrix> for relevant services and protocols which need to be enabled in test suites.

Verification

No services are affected by the vulnerability scans so BSC is available for configuration and monitoring during scan. Also one call must be made successfully.

If serious vulnerabilities are found you must notify responsible person found at Problem mitigation plan.

Results, see Impact analyses

IMPACT ANALYSES

<HW variant>

List the amount of found vulnerabilities. If high vulnerabilities are found make the entry to Problem mitigation plan.

Level	Number of findings
High	
Medium	
Low	

PROBLEM MITIGATION PLAN

Who to connect for problem correction in following situations: unnecessary port open or platform / software vulnerability.

Notify Program manager on problem situations.

Problem reporting through normal procedures.

List of found vulnerabilities in BSC. List type of attack, the initial effect, the desired effect.

APPENDIX A

<HW variant> <Software main branch><Revision>

Test tool configuration

<list enabled plugins and versions>

APPENDIX B

<HW variant> <Software main branch><Revision>

Device configuration

Should be same as defined in Customer documentation.