Learning Diary:
Practical Internet Security

Tobias Glocker
University of Vaasa
Tobias.Glocker@uwasa.fi
Student Number: p87915

October 16, 2011

1 INTRODUCTION

Internet Security plays an essential role in our society. From year to year the number of break-ins in computer networks rises. Companies that became a victim of espionage or sabotage do not mention it in the publicity because they do not want to loose their reputation. Internet Security is not only important for companies but also for private persons that use the Internet in order to pay their bills. To reduce the risk of becoming a victim, it is recommended to use software that protects the computer from these threats. A lot of research has been done to ensure secure connections over the Internet. Nowadays Internet Security is a good business for companies that provide services for protecting computers against attackers and for establishing secure connections over the Internet.

2 PRACTICAL IPv6 SECURITY ISSUES

The first Internet Protocol Version 6 (IPv6) test was done in the year 1997. In the year 2000 the first tunneled IPv6 over Internet Protocol Version 4 (IPv4) was created. There is no identical topology between IPv6 an IPv4 due to some hardware and software limitations in routers or firewalls. In comparison to the IPv4, IPv6 has a bigger address space, a new header format with header extension through daisy chaining, a fixed base header (40 bytes) and a minimum Maximum Transfer Unit (MTU) of 1280 bytes. IPv6 provides a maximum packet size of 4 GB with Jumbo Payload Extension Header. The header of IPv6 does not contain a field for the checksum. Furthermore, the Address Resolution Protocol (ARP) was replaced by the Internet Control Message Protocol Version 6 (ICMPv6) that manages all "support functions". In order to guarantee secure communications the Internet Protocol security (IPsec) is mandatory in IPv6. IPsec provides network-level peer authentication, data origin authentication, data integrity, data confidentiality, and replay protection. Every interface has at least one IPv6 that can be assigned manually, through Stateless Address Autoconfiguration (SLAAC) or with Dynamic Host Configuration Protocol Version 6 (DHCPv6). In an IPv6 network routers can be configured manually or through a Router Advertisement (RA). According to Minoli (2006) a RA is a "[n]eighbor discovery message sent by a router in a pseudo-periodic way or as a router solicitation message response. The advertisement includes, at least, information about a prefix that will be used later by the host to calculate its own unicast IPv6 address following the stateless mechanism". Many Operating Systems use IPv6 as soon as a RA is received. (Vartiainen 2011.)

3 MOBILE PLATFORM SECURITY

By the year 2015 there will be five billion global mobile subscribers in the world. Every user would like to use his phone without being worried about the user assets (privacy), corporate assets (confidentiality) and the service provider assets (availability & authenticity). For that reason, security plays an essential role and the question comes up of "[h]ow to make sure your business is having feasible reliability and adequate share of the responsibilities?". (Puranen 2011.)

According to Puranen (2011) many definitions for product security exist and can be defined as follows.

- A product does what it is designed to
- Security is a process, not a product

- Product security is the incorporation into anything that Nokia productizes via security-related design, architecture, process, development, testing, release and maintenance
- Product security requires extra robustness and resistance for attacks against all parts of the architecture and functionality

One of the key questions is how a trusted service can be ensured. There are many opportunities in order to achieve a trusted service. One opportunity is to provide a perfect hardware security. Another possibility is to offer a high application security with strong data encryption. Furthermore, the Operating System security, the usability and the software update capability play an essential role. Besides the security features, a higher trust could be reached by providing an excellent user manual. The main problem of getting trust is that a lot of money and time need to be invested. **Figure 1** shows how the security levels are matched with the product life cycle in the business case.

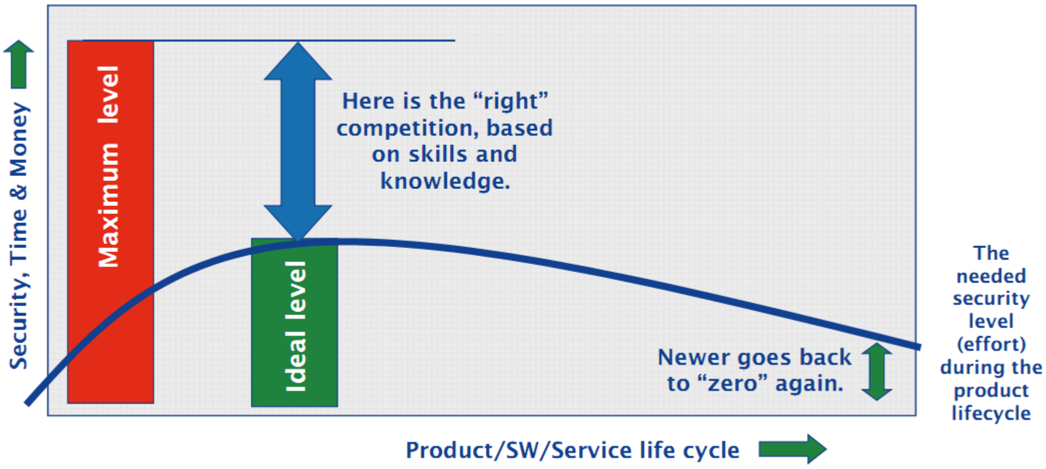
Security, Time & Money
Maximum level
Here is the "right" competition, based on skills and knowledge.
Ideal level
Newer goes back to "zero" again.
The needed security level (effort) during the product lifecycle
Product/SW/Service life cycle

Figure 1. Matching Security Levels With Product Life Cycle. (Puranen 2011.)

Reaching the maximum security level requires a lot of time and money. The costs should be reasonable to the products life cycle. For that reason an ideal security level should be found that guarantees a certain security until the expected lifetime. (Puranen 2011.)

4 DNSSEC: PRACTISES & DEVELOPMENT

Domain Name Service (DNS) is a hierarchical, distributed and redundant database. It is one of the most essential services in a network. To its main task belongs the answering of requests regarding to name resolution. DNS makes it possible to communicate between names because for humans it is easier to memorize host names instead of Internet Protocol (IP) addresses. If a user wants to access the google website it is easier to type "www.google.com" instead of "209.85.148.99". As already mentioned the DNS is a hierarchical, distributed and redundant database. Hierarchical means that the name resolution (www.google.com. ,for example) starts from root ("."), then ".com", then "google" and so on. It is also called a distributed database because each zone (for example .com) can be administrated and hosted independently. DNS is also redundant. There are so called "Authoritative Slave Servers" that are synchronized with the Master Server. In case one server stops working DNS is still active. A further advantage is that the traffic can be balanced between the servers. (Migault 2011.)

Migault (2011) showed in his presentation that Internet Service Providers rely on DNS because it provides all the services that are needed when accessing the Internet. For that reason a DNS must have the following properties.

DNS Service must be efficient:

- DNS Resolution is part of the Internet access service
- DNS Authoritative Servers is part of the services efficiency ISPs provide
- DNS manages the ISPs' network (load balancing, service redirections etc.)

DNS Service must be trusted when private information is involved:

- login, passwords, authentication, mails, photos etc.

In computer networks there is always the risk of networks attacks. A DNS attack could have serious consequences. An attacker could steal a Fully Qualified Domain Name (FQDN) with Domain Name Hijacking (DNHJK). As soons as the attacker has control over a Domain Name the attacker can redirect the traffic to a web site that hosts malwares, a merchandised website, a faked web site for identity theft or to an alternative server to isolate a web site. In order to avoid DNHJK attacks a secure DNS is needed. A secure DNS can be build with the Domain Name System Security Extensions (DNSSEC) that were first specified in March 1997 and finalized in March 2005. The developed DNSSEC uses a public key to identify authoritative zones. This key is called Key Signing Key (KSK). In DNSSEC all answer are digitally signed so that a DNS resolver is able to check if the received information was sent from an authoritative DNS server. (Migault 2011.)

5 MALWARE TECHNIQUES TODAY

The first known PC boot sector virus was called Brain and was discovered int the year 1986. This virus infects the boot sector of a storage media formatted with the File Allocation Table (FAT) file system. It replaces the boot sector of a floppy disk with a copy of the virus. In other words it moves the original boot sector to another sector, marked it as bad and changes the disk label to ©Brain. When reading the infected boot sectors the following text can be seen:

"Welcome to the Dungeon (c) 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!"
(Tikkanen 2011.)

To malware belongs beside computer viruses also Trojan horses. Tikkanen (2011) introduced in his presentation the powerful Haxdoor Trojan. Haxdoor is capable to backdoor Trojans that gather private user data and send them to remote attackers. The data sent to the attacker might include credit card numbers, logon credentials for banks as well as user names and passwords. It can also disable security-related software and may perform malicious actions.

The demos given during this presentation clarify the effects of malware. To reduce the risk of becoming infected with malware it is wise to have an updated security software installed on every computer.

6 SECURING BGP

The Border Gateway Protocol (BGP) is "[a] protocol from better times". It is a protocol from the early Internet. At that time people were more friendly and trustworthy. One of the main assumptions for this protocol is that routers do not lie.

BGP can be described as a path vector protocol that makes routing decisions based on path or according to a network policy. Since BGP does not use the traditional Interior Gateway Protocol (IGP) metrics it is more a reachability protocol than a routing protocol. According to Donnerhacke (2011) the following threats can appear in BGP.

Fat fingers
 - Announcing wrong network
Broken devices
 - Bitflip in memory or transit
Commercial/criminal attacks
 - Redirect traffic (claim prefix, claim peering)
 - Inject unallocated networks (sending Spam)
Governmental/Lawful attacks
 - Filtering traffic to protect the innocent

In order to avoid the previous mentioned threats, a Secure BGP (S-BGP) has been developed. S-BGP establishes a public-key infrastructure that uses digital certificates to authenticate the data. (Donnerhacke 2011.)

7 CONCLUSION

In this seminiar we learned a lot about Malware, IPv6 Security, DNSSEC and Secure BGP. All of the taught contents are essential for todays and tomorrow's Internet Security. The demos presented during the presentation of "Malware Techniques Today" showed, what could happen if a computer gets infected with a virus or Trojan horse. Furthermore, it was interesting to hear how DNS works, what are the threats of DNS and how a secure DNS could be build. The laboratory exercise on the second day deepens the knowledge learned in the presentation "DNSSEC: Practises & Development". Another interesting part in this seminar was to see the differences between the IPv6 protocol and the IPv4 protocol and how to make BGP secure. The content of the "Mobile Platform Security" presentation covered essential topics that are relevant for mobile devices.

8 BIBLIOGRAPHY

Donnerhacke, Lutz (2011). Securing BGP. Large scale trust to build an Internet again. INFORTE Seminar Presentation.

Migault, Daniel (2011). DNSSEC: Practises & Development. INFORTE Seminar Presentation.

Minoli, Daniel (2006). *Voice Over IPv6. Architectures for Next Generation VoIP Networks.* Elsevier Inc.

Puranen, Kimmo (2011). Mobile Platform Security. A Standards-Based Approach. to Securing Mobile Computing Devices, Software, and Applications. Senior Product Security Technology Manager. Nokia CTO Office, Product Security. INFORTE Seminar Presentation.

Tikkanen, Antti (2011). Malware Techniques Today. F-Secure Labs. INFORTE Seminar Presentation.

Vartiainen, Tuure (2011). Practical IPv6 Security Issues. Tampere University of Technology. INFORTE Seminar Presentation.