UNIVERSITY OF VAASA

FACULTY OF TECHNOLOGY

TELECOMMUNICATIONS ENGINEERING

Arto Mäenpää

INFORMATION SECURITY FOR BYOD IN ABB

Master´s thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 2 September, 2013.

Supervisor	Professor Mohammed Salem Elmusrati
Instructor	Tobias Glocker

ACKNOWLEDGEMENT

This thesis has been made in the information security department of ABB. Making the thesis has been quite a journey for me personally and I never would have made it without the support of those who believed in me throughout this whole experience. There are a lot of people who I should thank a lot for being there for me but particularly the big thank you goes to my girlfriend Minna who has been really supportive towards me during these hectic times as well as for Tobias Glocker who was always there when I needed some help related to work. I would also like to thank my parents who have helped me financially during the time I have been studying. So big thank you to you as well!

Arto Mäenpää

Table of Contents

ABBREVIATIONS

3DES	Triple DES
AES	Advanced Encryption Standard
ARM	Advanced Risk Machines
BIOS	Basic Input Output System
BYOD	Bring Your Own Device
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
DES	Data Encryption Standard
FTP	File Transfer Protocol
HLR	Home Location Register
IETF	Internet Engineering Task Force
IN	Intelligent Network
IOS	Internet Operating System
ISP	Internet Service Provider
OSI-model	Open Systems Interconnection Reference Model
OTP	One-Time Password
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
SAEM	Security Attribute Evaluation Method
SSH	Secure Shell

USB	Universal Serial Bus
UWYT	Use What You Are Told
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

UNIVERSITY OF VAASA

Faculty of technology

Author:	Arto Mäenpää
Topic of the Thesis:	Information Security for BYOD in ABB
Supervisor:	Mohammed Elmusrati
Instructor:	Tobias Glocker
Degree:	Masters of Science in Technology
Degree Programme:	Degree Programme in Telecommunications Engineering
Major of Subject:	Telecommunications Engineering
Year of Entering the University:	2005
Year of Completing the Thesis:	2013 **Pages:** 98

ABSTRACT

BYOD (Bring Your Own Device) is the future policy in companies that is going to replace the old UWYT (Use What You Are Told) way of thinking. This new policy has a lot of issues both security wisely and policy wisely that needs to get solved before we can fully implement this policy into larger companies. Thanks to large interest in the subject a lot of companies have already come up with solutions to this issue and started to use BYOD policy within their companies.

The main target of this Master´s Thesis "Information Security for BYOD in ABB" was to create a working information security system for future BYOD policy use in ABB. For the Thesis we used six different test users with different portable devices and statuses and tried to create a policy that fits well with their job and fulfills the security requirements of ABB. We also discuss a little about cloud computing and how it is good to be included into the final solution for the BYOD security plan.

KEYWORDS: BYOD, Information Security, ABB, Security Planning

1. INTRODUCTION

In the consumerization of IT, bring your own device (BYOD) is a phrase that has become widely adopted to refer to employees who bring their own computing devices such as laptops and smartphones into their working place and use them to access the corporate network and corporate data. Today employees expect to use personal smartphones and mobile devices at work and a lot of companies have started to implement BYOD security policy within their companies. For example the IT may require that the mobile devices are configured with passwords, only certain applications are allowed and that the data on the device must be encrypted.

The main goal of this thesis is to develop an information security plan for BYOD use in ABB for the information security department. Being the leading company in power and automation technology ABB invests a lot of money into research and development. Because for example in the graphics area Apple products have become more and more popular among the employees it would be good for ABB to also allow the development workers to bring their own iMac laptops with them into their working place. IMac´s processor is more efficient and it runs and compiles the graphics more efficiently. That is why it has become more and more popular among the designing people (see **Figure 1**). If the employees get allowed to use their own devices at work it is vital for ABB to come up with a secure plan how to protect the corporate network from threats and attacks as well as creating a policy for the mobile devices that is legal and secure here in Finland.

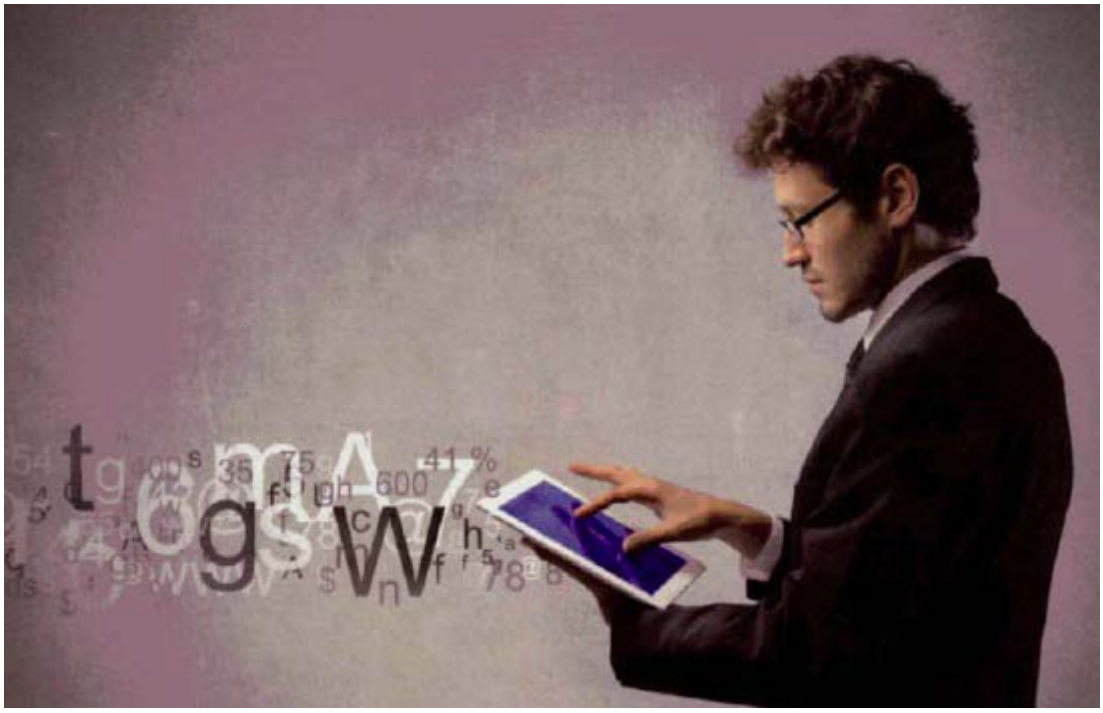

Figure 1. Employee using iPad for designing (Niharika 2012: 5).

The thesis consists of six chapters where the first chapter contains the introduction to the thesis. In the second chapter the company structure and the history of ABB are explained. Chapters three and four are theoretical parts of bring your own device (BYOD) sharing some information about the whole concept and its advantages and disadvantages. It also contains important information that what needs to be taken into consideration while creating a safe BYOD solution and policy for ABB. In the fifth chapter there is a BYOD solution which contains both policy solution, solution model for the different internet operating systems as well as interviews from the employees of ABB about their pilot BYOD devices. The conclusion part can be found in the chapter six with future suggestion for ABB about the whole concept.

2. HISTORY OF ABB AND CURRENT LANDSCAPE

ABB is a global leader in power and automation technologies. It is a multinational corporation which has its headquarters based in Zurich, Switzerland. The company operates in approximately 100 countries and has over 145,000 employees (June 2012). ABB´s current form was created in 1988 but it´s history spans over 120 years. It´s business is comprised of five divisions that are organized in relation to the customers and industries they serve. The success of the company has been driven particularly by a strong focus on research and development. The company has seven research centres around the world and it has a long track record of innovations. Many of the modern society inventions from high-voltage DC power transmission to the revolutionary approach to ship propulsion were developed by ABB. Today ABB is the largest provider of generators to the wind industry and the largest supplier of power grids worldwide. In **Figure 2** a data centre in ABB Sweden is represented. (ABB Intranet 2013.)

Figure 2. ABB data center in Västerås, Sweden (ABB 2012).

2.1. Corporate architecture

The corporate architecture of ABB consists of five different divisions; Power Products, Power Systems, Discrete Automation and Motion, Low Voltage Products and Process Automation. The Power Products division is the largest one with over 36 000 employees and it consists of three business units: High Voltage Products (PPHV), Medium Voltage Products (PPMV) and Transformers (PPTR).

The second largest division is Low Voltage Products which has about 31 000 employees. The main business units in Low Voltage Products are Breakers and Switches (LPBS), Control Products (LPCP), Enclosures & DIN-Rail Products (LPED), LV Systems (LPLS), Thomas & Betts (LPCW) and Wiring Accessories (LPWA).

Discrete Automation is the third largest division in ABB with over 29 000 employees. It consists of four business units including Drives and Controls (DMDR), Motors and Generators (DMMG), Power Conversion (DMPC) and Robotics (DMRO).

Process Automation has about 28 000 employees and it is almost equally as big as Discrete Automation division. It contains nine different business unites including Control Technologies (PACT), Full Service (PAFS), Measurement Products (PAMP), Marine & Cranes (PAMA), Mining (PAM), Oil, Gas and

Petrochemical (PAOG), Paper, Metals & Cement (PAPM), Service (PASV) as well as Turbocharging (PATU).

The smallest division with over 20 000 employees is the Power Systems. It contains four business units Grid Systems (PSGS), Network Management (PSNM), Power Generation (PSPG) and Substations (PSSS). For Power Systems the key deliverables are AC and DC power transmission grid systems for traditional and renewable energy integration, network management and systems, turnkey substations (including substation automation) and power systems services. **Figure 3** represents the most important innovations ABB has been involved with. (ABB Intranet 2013.)

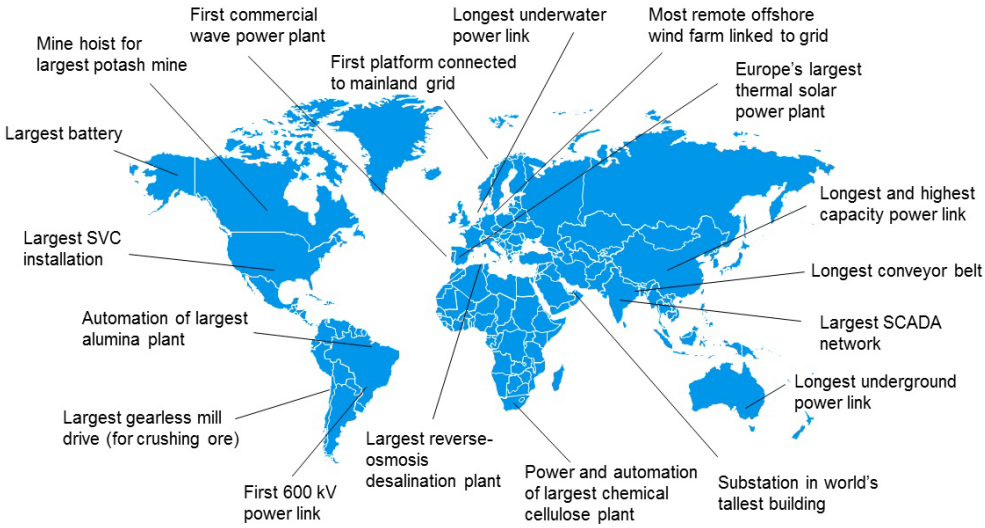

Figure 3. Some of the most important inventions done by ABB worldwide (ABB group presentation 2013: 11).

2.2. Information systems governance

This chapter of the thesis contains confidential information about the structure of information security in ABB and it is thus removed.

3. BYOD

Chapter three consists of BYOD. In first section the BYOD concept is described and compared to the old UWYT (Use What You Are Told) policy. After going through the differences between the two concepts the main advantages and disadvantages of BYOD are described. On the last section of the chapter the BYOD privacy considerations are briefly described.

3.1. BYOD Concept

Figure 4. Different BYOD devices (Jain 2012).

BYOD (Bring Your Own Device) (also referred to as Bring your own technology (BYOT), Bring your own phone (BYOP) and Bring your own PC (BYOPC)) is a recent trend that has been observed in many companies where the company employees bring their personally-owned mobile devices, iPad's or laptops to

their workplace to access corporate resources such as email, databases, file servers as well as their own personal data. The policy was first discovered in 2009 by Compared to the old way of thinking UWYT (Use What You Are Told). It is a more flexible concept and gives the employee opportunity to choose the device what fits best for his job. Using personal devices (see **Figure 4**) at work is beneficial for the companies because it gives the employee's freedom to choose the device that fits best for their needs and it increases productivity and flexibility within the company. Even though BYOD has been considered beneficial for the company because it raises the happiness and productiveness of the employee, it´s policy contains some data security risks. In **Figure 5** can be seen the main differences between the BYOD and UWYT – concepts from the employee perspective. BYOD is much more flexible concept but it also requires a higher technical ability from the employee than UWYT. It requires more training for the employee and also a clear policy what the employee is allowed to do with the device and what not. In UWYT the information security is "tightly coupled" within the company and there is a control of all layers of architecture. The BYOD policy depends what kind of agreement the employee and the employer have made about the applications, devices and security issues. The devices in UWYT – companies are always centrally supported by antivirus and data protection but in BYOD the data protection is divided into internal protection for the data and external protection for the endpoint user. (Burt 2011: 1.)

The information and data flow oversight in BYOD is much less controllable than in UWYT where everything what is done with the company´s own device can be controlled. In BYOD the concept allows the employee to install their own

software to the computer and because of that also the data leakage is more likely to happen in BYOD compared to UWYT. There is also a big question about the data and ownership of the device. The biggest question from the bringing your own device is if it is owned by the employee or if it is owned by the company? This is an important question because it must be clarified if the company is responsible for buying a new one to the employee and allowed to wipeout the stolen computer or if the employee just buys a new one and hopes that the data from the stolen computer won´t end in wrong hands? (Burt 2011: 1.)

	UWYT - Employer	BYOD - Employee
Information Security Governance	Standardized endpoints with a Block or Disregard policy approach – "tightly coupled" control of all layers of architecture – focus on corporate control – this is a corporate liable model	Move to a 'loosely coupled' approach to endpoint management. This is not a endpoint centric approach – focus on policy, culture change and controlling the applications, systems and information layers – requires a BYOD policy to be in place describing responsibilities of employer and employee – this is a blend of a corporate and individual liable model
Operations	Centrally supported data and endpoint service, standard security, antivirus and data protection – requires an acceptable use policy but no mention of personal endpoints	Expands the scope of support to hybrid model – internal for data, external vendor for endpoint, distributed security, antivirus and data protection
Personnel	Lesser level of employee technical ability due to central support, no tax implications as these endpoints are considered equipment, standard user experience and support. Lower costs to create and deliver training on standard endpoints	Higher level of employee technical ability due to hybrid support, stipend model may result in income tax implications; potential confusion for users resulting in unsatisfactory service, a BYOD policy must be created. Higher costs to create and deliver training
Information and Data Flow	Centrally provisioned and secured information to meet regulatory and compliance rules and audits. Access controls limit data leakage based on information classification methods	Leverages centrally provisioned and distributed security, need an ability to wipe enterprise data but not personal data, more controls required to meet regulatory and compliance rules and audit – digital rights management
Application	Entire application infrastructure contained to corporate endpoints to limit vulnerabilities and data leakage. Provides employees with only the applications they need and typically with a lesser user experience	Focus on open standards that will run on any endpoint; consideration for future applications (buy or build); strategies needed to separate personal apps from enterprise apps due to the possibility of inappropriate data access
System	Centralized control of access to applications, systems and information using IAM and PKI security, IT	Strong reliance on HR business processes to timely notify of changes in employee status; IAM is a critical

Figure 5. Differences of UWYT - employee and BYOD - employee (Niharika 2012: 2).

Cisco System´s annual Visual Networking Index Forecast predicted in June 2011 that there will be over 15 billion network-connected devices including smartphones, notebooks, tablets and other smart machines in 2015. (Jeffrey 2011: 1.) The usage of personal PC, smartphone and tablet in business applications has increased by 10% between 2010 to 2011. This clearly shows that the demand for BYOD in larger companies is coming even higher in the future because the network-connected devices are becoming more and more common within the employees. In the following two sections the advantages and disavantages of BYOD are discussed more briefly. (Burt 2011: 1.)

3.1.1. Advantages of BYOD

There are several advantages and disadvantages of BYOD policy which will be discussed in the next two chapters. The biggest advantage in BYOD compared to UWYT policy is that the employees are much happier, productive and collaborative when they can bring their own devices to work. According to a survey made by iPass of 1,100 mobile workers, it was figured out that the employees who used mobile devices for both work and personal issues worked 240 hours more per year than those who don´t have their own mobile working devices. BYOD also reduces the costs in maintenance because employees will have to take care of the hardware and software by themselves instead of some company employee handling them for all. In larger organizations such as ABB it is also quite impossible to keep the hardware and software always up-to-date but with BYOD the employee himself can update it fast in order to decrease the security threats. (Niharika 2012: 4.)

BYOD can also be seen as a competitive advantage over other companies. It attracts best employees because they know that within the BYOD company they can have flexible working hours and they can also work at home after the working hours if necessary. This of course increases the engagement of the employees to work in after hours and it is always beneficial for the company. BYOD can be seen more as a business decision than an IT decision. By embracing BYOD the organization gets benefits from having a more productive and collaborative end user environment, the ability to retain and hire highly talented people for end users and give them more flexibility. (Niharika 2012: 4.)

3.1.2. Disadvantages of BYOD

Even though BYOD has been considered as a positive policy for the companies it also has a lot of disadvantages as well. When an employee attaches his personal smartphone or tablet to an organizational network or machine, it makes sense to worry about the overall security. When the external devices are attached, malware could immediately migrate from the personal device to the company´s machines and over corporate network. Also when the employee is allowed to access the corporate network it is likely that the sensitive data will also end into the employees own personally used device. This data could include for example customer information or company information that should be kept private. When that kind of information is carried away from the company on a daily basis, bad things can happen especially if the device is stolen or lost. (Miller, Voas & Hurlburt 2012: 2.)

When laptops became more common people were as afraid what will happen as they are now with BYOD. They are larger than smartphones with higher memory capacity so when a laptop disappears it is more likely to be noticed. Another big and less physical aspect is that when the company is using its own laptops and devices, it usually enforced its own policies to those machines requiring passwords and encrypted the sensitive data. Usually the devices are this time owned by the employee and it makes it harder for the company to enforce their own policy into the devices which they actually don´t even own. If the device is owned by the company it would become quite expensive for the company because then they would have to buy for the employees all the devices they think they need in their personal and work use. This is a key factor that needs to be understood completely before applying the BYOD policy in the company. (Miller, Voas & Hurlburt 2012: 2.)

The employees using BYOD need to be more experienced than the employees working with the UWYT devices. They need to be well aware about the risks that can occur when they for example install an application that is used for personal purposes only. To keep the employees updated about the latest threats they need to be trained more and it will cost money for the company. (Miller, Voas & Hurlburt 2012: 2.)

For the company another thing to be worry about, is the lack of uniformity and compatibility issues. Some applications and tools may not be uniform on all devices and it can result in incompatibility when for example trying to connect

to the corporate network or access a word file created by another employee who has purchased a newer version. (Priyadarshi 2013.)

Depending on the solution whether the employee saves the company´s data while working to a cloud or directly to the corporate network can also be a risk factor for the company. If the data is stored into cloud the cloud needs to be partitioned and protected so that the employee can´t access other partitions in the cloud or a third party gets access to the company´s sensitive data. The employee also needs to secure the Internet connection because the company isn´t securing it for them. (Miller, Voas & Hurlburt 2012: 3.)

3.1.3. BYOD Policy Considerations

Even though the security seems to be the major concern when companies and people are discussing about BYOD and BYOT, the issue of privacy seems overlooked and potentially more important. The policy in BYOD must follow both the company policies as well as the national policies, so the companies' aren´t allowed monitoring every move the employee does in his free time. Mobile devices and laptops can contain a lot of data that the employee wants to maintain private and if the laptop also contains company data, how can the barriers be set in such a way that it is legal? In BYOD also the organizational control over data is blurred. When business and private data exist on the same device it can cause a lot of problems because some applications may require license for business use but for private use they are free. (Miller & Voas & Hurlburt 2012: 3.)

3.2. Cloud computing

Figure 6. Different devices in cloud computing (Ramsey 2013).

Internet can generally be seen as a collection of clouds as you can see from the **Figure 6**. This means that the cloud computing is a set of resources and services that are offered through the Internet (Shaikh & Haider 2011: 2). Cloud computing enables consumers to access resources online through the Internet. The resources from the cloud can be accessed at any time and from any place where an Internet connection is available. For creating a secure BYOD environment cloud computing is one good option because it is very cheap to setup and the maintenance doesn´t cost anything. It is cheaper than most of the other options to choose from and using a private cloud for the data storage makes the system more secure because the employee doesn´t have direct access to the corporate network. The biggest cloud service providers are Amazon and Google. Cloud services can be divided into three sections: SaaS (Software as a Service), PaaS (Platform as a service) and IaaS (Infastructure as a Service). These services and their structures will be discussed more briefly in the next sections. (Salmio 2012: 3.)

Platform as a Service (PaaS) is a service model where the user uses development tools and application development platforms over the Internet. In the model the user basically just writes the code, uploads it to the application development platform and runs it. The service provider offers the efficient development and testing environment and takes care of the maintenance. User only has to have an Internet connection and a browser to upload the software.

Most of the service providers in this area limit their development platforms so that it works only with certain programming languages. Some examples of the common programming languages used in cloud computing are Java and Python. The biggest service provider in PaaS is Google´s App Engine (GAE) which supports Java and Python as well as Google´s own programming language Go. (Salmio 2012: 15.)

The main idea in **Software as a Service** (SaaS) is that the clients use the service providers programs over the Internet. The services are located in the service providers servers so that the users using the services don't have to install any applications into their working spaces. The users only need a working browser (Internet Explorer, Mozilla Firefox, Opera, Google Chrome etc.) and an Internet connection to make the SaaS work. The service providers will take care of the maintenance, updates, help desk as well as about the information security of the service. The main advantage in SaaS is that it is easily reachable and usually the users only pay how much they use the service so it is also a very efficient and a flexible solution. (Salmio 2012: 14.)

Infastructure as a Service (IaaS) is the third service model which offers the users virtualized hardware as well as for example free space to store their data. Users can install and control their own operating systems and applications into the virtual hardware but the cloud infrastructure is controlled only by the service provider. IaaS is a very good choice for young companies because it is very efficient and cheap solution. It is much cheaper for the company to move the infrastructure into the cloud instead of buying their own workstations and servers. Usually the companies are paying from the amount of data they store into the cloud so it is a cheap solution when they aren´t paying anything from the free space. IaaS services are provided by for example Amazon, IBM and Microsoft, for example. The most popular IaaS services are Dropbox, Amazon Simple Storage Service and Amazon Elastic Compute Cloud. (Salmio 2012: 15.)

The lowest layer of the service models is IaaS because it offers the hardware which is a condition to make the upper layers work. In the middle is PaaS which offers a development platform to the highest level applications and the highest level is SaaS. Before the service models came the service provider and the servers and after the models the user using them. **Figure 7** shows a service model architecture in Cloud computing. (Salmio 2012: 15.)

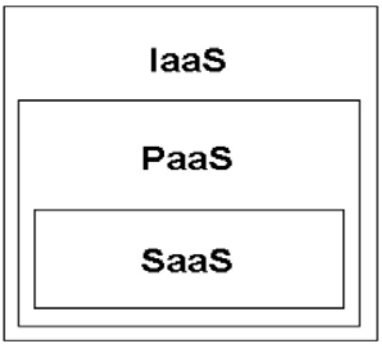

Figure 7. Service model architecture in Cloud computing (Salmio 2012: 16).

3.3. Virtual Private Network

A virtual private network (VPN) is a private network constructed within a public network infrastructure, such as the global Internet. A VPN provides network-to-network or remote-user-to-network connectivity via an encrypted tunnel through the public Internet. VPN is widely used in international companies where the offices are far away from each other but they still have a main office and main server for data storage. In **Figure 8** you can see a basic concept of VPN connection over Internet. (Innanen 2003: 3.)

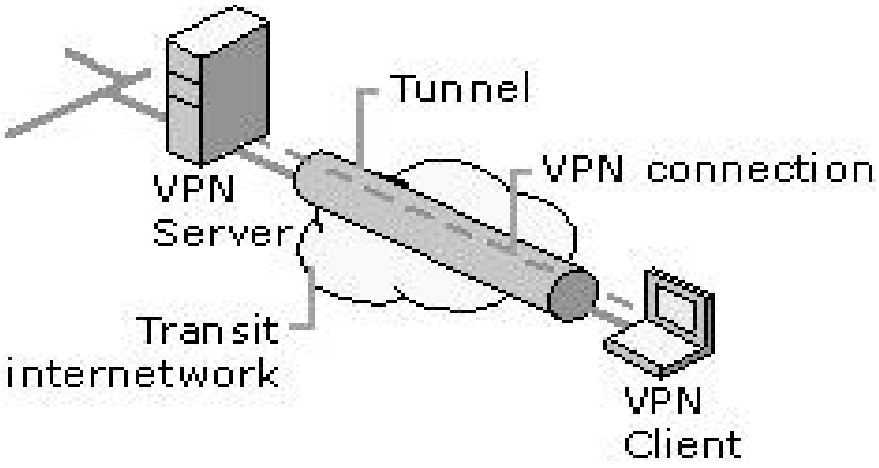

Figure 8. Basic concept of VPN over Internet (Innanen 2003: 3).

VPN connections can be divided into three categories: trusted VPN, secure VPN and hybrid VPN. Trusted VPN is the oldest one of the connections and its roots are from the time where Internet started. At that time the Internet service provider (ISP) reserved the client a line that was only reserved for that client´s usage. These loaned lines were used as they were the clients own lines. At that time the privacy and protection of the line was only based on the ISP´s own words. Soon after the ISP´s started to develop a better connection and a secure

VPN was developed, which shares information between two line using encryption. Hybrid VPN is a result of combining secure VPN and trusted VPN together. Remote user VPN can be seen in the **Figure 9**. It is almost similar to normal VPN connection but it has a company firewall protecting the intranet. (Innanen 2003: 3.)

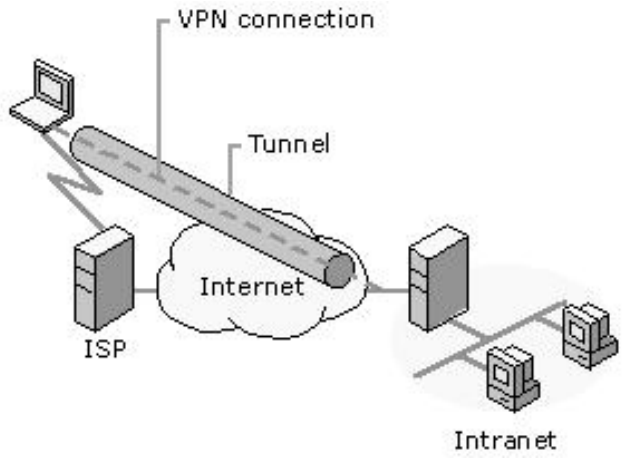

Figure 9. VPN connection for remote user (Innanen 2003: 4).

3.3.1. VPN Tunneling

The basic idea of tunnelling in VPN is that the unprotected traffic is put inside a "tunnel" that protects it from the third party. Tunnelling requires special software to secure the connection for both ends. The connection between the client´s tunnelling software and tunnelling server is called tunnel. Tunnelling means that instead of direct connect first a connection with tunnelling software is made before the final connection to the client is established. Between the tunnelling software there is some own protocol used that first encrypts the

packages and then sends them to the end user. Before sending the data into the final destination the data is decrypted into its original form.

The tunnelling protocols are divided into either 2nd or 3rd layer protocols depending how they work in the OSI (Open Systems Interconnection) –model. The most common VPN protocols are IPSec (Internet Protocol Security), L2TP (Layer 2 Tunneling Protocol) and PPTP (Point to Point Tunneling Protocol). They will be explained briefly within the next sections. In **Figure 10** a typical VPN protocol architecture is presented. (Innanen 2003: 3.)

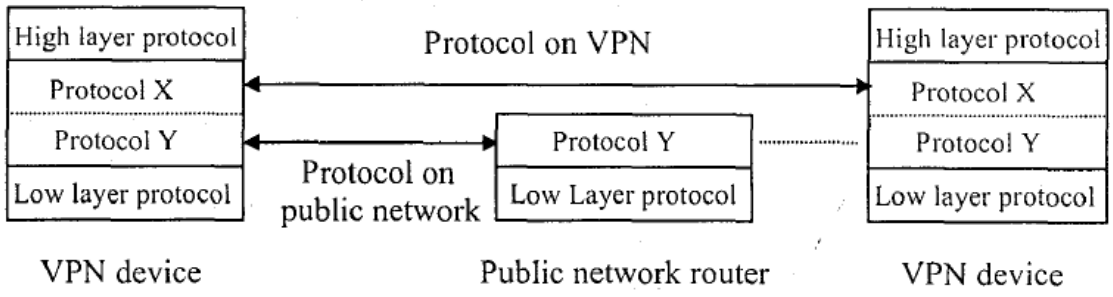

Figure 10. VPN protocol architecture (Aqun & Yuan & Yi & Guangun 2000: 3).

The IP Security (IPSec) protocol includes a series of standards proposed by IETF Internet Engineering Task Force) which introduce security mechanisms into TCP/IP network. The security protocols in IPSec include Authentication Header (AH), Encapsulating Security Payload (ESP), Security Associations (SAs), key management and security algorithms. The encapsulation form of IPSec in tunnel mode is (IP(AH or ESP)(IP))))). (Aqun & Yuan & Yi & Guangun 2000: 3.)

Layer 2 Tunnel Protocol (L2TP) could be classified as a tunneling protocol supporting Internet-based remote access and work on the data link layer of the OSI/RM architecture along with Microsoft´s Point to Point Tunnel Protocol (PPTP) and Cisco´s Layer 2 Forwarding (L2F). The form of L2TP packet can be seen below from the **Figure 11.** (Aqun & Yuan & Yi & Guangun 2000: 3.)

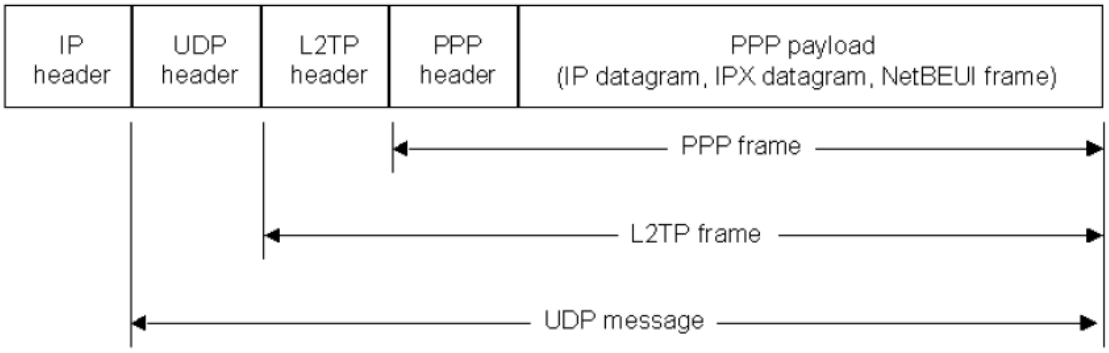

Figure 11. Structure of L2TP packet (Innanen 2003: 7).

Point to Point Tunneling Protocol (PPTP) was originally developed by Microsoft to its Windows NT servers. PPTP delivers PPP frames in IP-diagrams and transfers them over the Internet. PPTP can be used for combining routers together or by creating remote connections. In **Figure 12** a basic structure of PPTP packet is presented. (Innanen 2003: 6.)

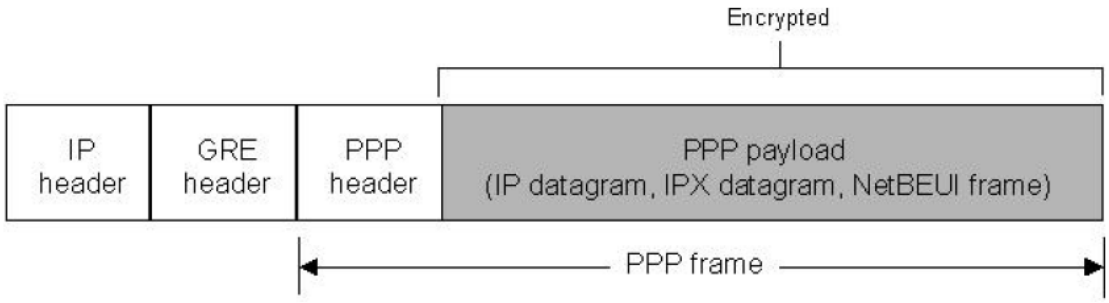

Figure 12. PPTP packet structure (Innanen 2003: 7).

3.3.2. VPN Data Encryption

Before the Internet data encryption was rarely used by the public. It was used in the military area. Today online shopping has become more popular and people are using their own bank accounts online thus it is essential to encrypt the data traffic. When sending data over the network it is always important to encrypt it with some algorithm. The main idea of data encryption is to transform plaintext into cypher text in a way that is non-readable to unauthorized parties. In VPN there are several different encryption methods to handle the data encryption. They are usually divided into two categories: symmetric and non-symmetric algorithms.

In symmetric encryption the sender and the receiver share the same secret key. The same key is used for the encryption and decryption. The longer the key length is the more secure is the encrypted data. The usage of the same secret key for both sender and the receiver are fast and efficient ways to send data over the VPN. The most common symmetric algorithms are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES). DES is the oldest encryption standard with only 64-bit encryption. Because the symmetric algorithms are based on the same keys, they can be cracked if the calculation speed of the computer is high. DES encryption uses only 64-bits for encryption and for that reason it has mostly been replaced with either 3DES or AES algorithms. 3DES is an advanced algorithm from DES. It uses two or three 56-bit encryption keys to create the algorithm so it is using either 112 or 168 bits for the data protection. AES is the

strongest and most popular algorithm from these three containing 128, 196 or 256 bit secret key. (Torro 2007: 26.)

In non-symmetric algorithms the sender and the receiver are using key pairs where the other key is public and the other key is secret. The keys work in a way that if the data is encrypted with a secret key it could be decrypted with the public key and if the data is encrypted with the public key it could be decrypted with the secret key. Because of the usage of two different keys it is almost impossible to crack the algorithms within a short amount of time and this makes the data sent over the network secure. This is also the weakness of the system because it takes so much time for the algorithm to get the data encrypted and decrypted. The two most commonly used non-symmetric algorithms are **RSA, ECC** (Elliptic Curve Cryptography) and **Diffie-Hellman**. RSA fractionises large numbers into its prime factors. It has become the most popular non-symmetric algorithm because it is so simple to create. The formula for creating an RSA algorithm is:

(1)

Where M is the message being encrypted, C the encrypted message and e the public key. For decrypting the message following formula should be used:

(2)

When decrypting the message d is the secret key. The only thing that remains the same in both encryption and decryption is n. (Torro 2007: 26.)

Most of the products and standards that use public-key cryptography for encryption use RSA. When the computers have become more efficient and the

calculation power has increased, the bit length for RSA has started to increase. This has increased the processing load on applications that use RSA. For electronic commerce sites that conduct large numbers of secure transactions this has already become a burden. **Elliptic Curve Cryptography** (ECC) which is a relatively new mechanism has started to challenge RSA. Unlike RSA, ECC is based on discrete logarithms which are much more difficult to challenge at equivalent key lengths. Compared to RSA ECC appears to offer equal security for a far smaller bit size, thereby reducing processing workload. (Stallings & Brown 2008: 645). An elliptic curve can be defined with the following equation:

(3)

From **Figure 13** can be seen an elliptic curve with the operation P + Q = R.

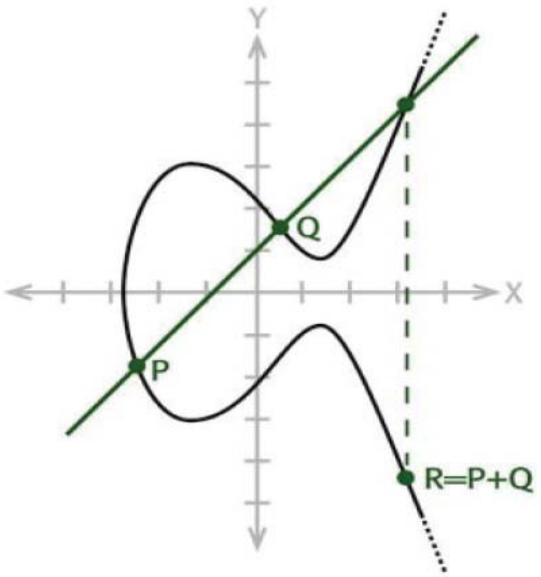

Figure 13. Elliptic curve showing the operation P + Q = R (Kapoor, Vivek & Singh 2008: 5).

The crucial property of an elliptic curve is that we can define a rule for adding two points which are on the curve to obtain a third point which is also on the

curve. The points and the addition law form a finite Abelian group. For addition of the two points also a zero point 0 is needed to be the point of the curve. It can´t satisfy the elliptic curve equation because otherwise it won´t work. The curve order is the number of distinct points on the curve including the zero point. After having defined the additional two points it is also possible to define the multiplication $k\mathbf{P}$ where k is a positive integer and **P** is a point as the sum of k copies of **P**.

If four persons A, B, C and D agree on a (non-secret) elliptic curve and a (non-secret) fixed curve point F. A chooses a secret random integer which is the secret key and publishes the curve point as the public key. B, C and D does the same like A. Now when we suppose that A wants to send a message to B. One way is to simply compute and use the result as the secret key for a conventional symmetric block (for example DES). B can compute the same number by calculating because

(4)

The security of ECC is based on the assumption that it is difficult to compute **K** given **F** and **KF**.

When choosing the fixed curve for ECC a finite field must first be chosen. If the field is for example GF(p) where p is a large prime number, the term xy is omitted, leading to the following equation:

+ a + b, where (5)

If the selected field is GF( ), then we include the xy term to get

(6)

Fields GF(with both p < 2 and m > 1 are not considered here.

After choosing the fixed curve we choose the fixed point. For any point P on a elliptic curve in the GF(,

(7)

For some *a* and *b*, b > a we will have a *a*P = *b*P. This implies cP = 0 where c = b - a. The least c for which this is true is called order of the point and c must divide the order of the curve. For good security the curve and the fixed point must be chosen in a way that the order of the fixed point F is a large prime number. With above provisions if F is an n-bit prime then computing *k* from *k*F and F takes roughly ⁻ operations. Equations based on elliptic curves are attractive because they are relatively easy to perform, and extremely difficult to reverse. **Table 1** shows a key-length comparison of ECC and RSA. It shows that ECC can create the same level of protection than RSA in smaller amount of bits. (Kapoor, Vivek & Singh 2008: 5.)

Table 1. RSA and ECC key-length comparison (Kapoor, Vivek & Singh 2008: 6).

Time to break (in MIPS-years)	RSA key-size (in bits)	ECC key-size (in bits)
10^4	512	106
10^8	768	132
10^{11}	1024	160
10^{20}	2048	210
10^{78}	21000	600

Diffie-Hellman algorithm is based on discrete logarithms. The effectiveness of the algorithm is based on the difficulty of computing discrete logarithms. The purpose of the algorithm is for two users to use exchanged secret key for encrypting messages. Discrete logarithm can be described briefly in the following way. First a primitive root of a prime number p is defined as one whose powers generate all the integers from *1* to *p-1*. That is, if *a* is a primitive root of the prime number p, then the numbers

, (8)

are distinct and consist of the integers from 1 through p-1 in some permutation. For any integer *b* that is less than *p* and a primitive root *a* of prime number *p*, one can find a unique exponent *i* such that

where $0 \leq i \leq (p-1)$ (9)

The exponent i is referred to as the discrete logarithm of *b* for the base *a,* mod *p*.

With this background we can define the Diffie-Hellman key exchange. To define the Diffie-Hellman key exchange two publicly known numbers are needed; a prime number *q* and an integer that is a primitive root of *q*. If users A and B wants to exchange the key first they need to generate random numbers x and y. After A selects a random integer < g and computes . Similarly B does the same by selecting a random integer and computes . Each side keeps the X value private and make the Y value available publicly to the other side. User A computes the key as and user B computes the key as . These two calculations will end up into the same result. As a result the two sides A and B

have exchanged a secret value. The security of the Diffie-Hellman key exchange lies in the fact that it is relatively easy to calculate exponentials modulo a prime but it is very difficult to calculate discrete logarithms. **Figure 14** illustrates a typical structure of the Diffie-Hellman algorithm. (Stallings & Brown 2008: 641-642.)

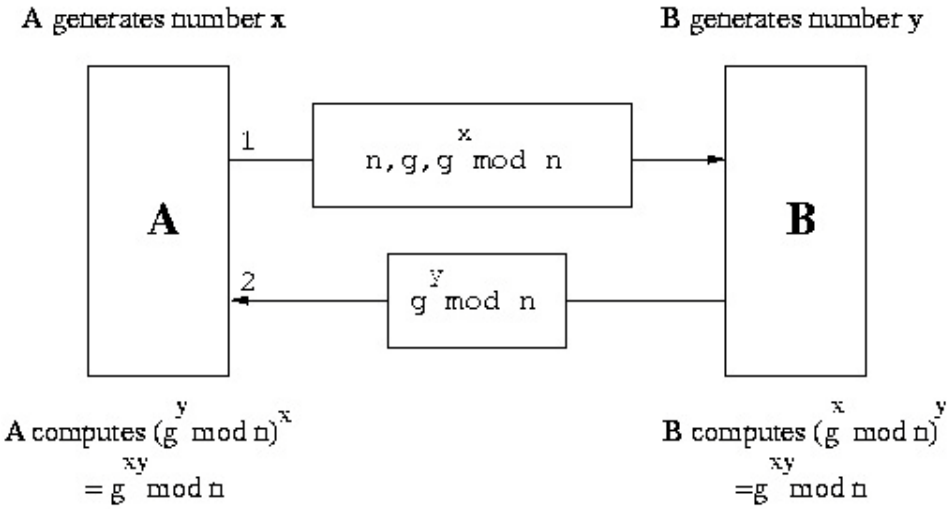

Figure 14. Diffie-Hellman algorithm.

3.3.4. VPN Authentication

Authentication is a process where the sender and the receiver make sure that both parties are what they claim to be. There are several different authentication protocols that can be used to authenticate a VPN connection. The most easy and unsecure solution for VPN authentication is the requirement of password and user name. For a more advanced and secure authentication public key

encryption is used. In the next sections the typical VPN authentication protocols and tokens are presented. (Huuhka 2011: 21.)

Password Authentication Protocol (PAP) is one of the oldest password –based authentication methods in remote access. It is based on the two-way handshake principle. First the remote user sends a login and password to the recipient. If the recipient types correctly the login and password, the server lets the user into the account. If the login or password is incorrect, it closes the connection and sends an error message. PAP authentication is weak because the data isn´t encrypted during the handshake and this can lead to a third party attack against the server. (Huuhka 2011: 20.)

Challenge- Handshake Authentication Protocol (CHAP) is a more advanced and secure authentication method than PAP. It is based on three-way handshake. In CHAP authentication while trying to connect to a server the user gets a message from the server which asks for login and password. The user password is protected for example with a MD5 – algorithm and combined with a hash value before sending it back to the server. The server then processes the hash value and if it matches the server's values, the user is accepted to connect to the server. CHAP is more secure than HAP because the authentication process is fully encrypted. (Huuska 2011: 21.)

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a little more advanced version from the traditional CHAP authentication protocol

and it is being used only in Windows systems. The difference between MS-CHAP and CHAP is that in MS-CHAP MD 4 algorithm is used for data encryption instead of MD 5. It also allows the user to save his password encrypted to the server. In CHAP the saved password isn´t encrypted so there is a possibility that someone could read it. (Huuska 2011: 21.)

Extensible Authentication Protocol (EAP) is an advanced version of the PPP (Point-To-Point) protocol that is working on the link layer. EAP guarantees wider support for different authentication methods such as Token-cards, single-use passwords, public key authentication as well as digital certification usage. There are many different versions of EAP which slightly differ from each other. These kind of protocols are for example Lightweigth EAP (LEAP), Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS) and EAP- Tunneled TLS (EAP TTLS). With LEAP authentication method you can secure wireless connections. In this technique the user authenticates first to the authenticator and then the authenticator identifies itself back to the user. In PEAP the authentication happens with digital certificates directly through the authentication server and user and there is no need for a separate authenticator. In EAP-TLS the authentication is based on user name and password. (Huuska 2011: 22.)

Another way to authenticate the users instead of using the existing protocols is to use different kind of tokens for the authentication. There are three different tokens based on authentication that the SecurID has to offer: hardware tokens, software tokens and OTP (One-Time Password) On-demand tokens. These

three different tokens are based on authentication methods that will be described briefly in the following three sections.

Hardware tokens offer a hacker-proof authentication which is easy to use and user authentication is efficient. Hardware tokens are based into RSA´s synchronizing technology which uses 128-bit AES-algorithm to create single-use authentication code, OTP (One-Time Password).

To get logged into the SecurID´s secured system the user has to combine his own PIN- code with the token´s generated authentication code. These two codes combined create a OTP which is used for user identification or authentication. If the SecurID system confirms the OTP, it allows the user to get access into the secured material. This method is used for example when getting money from an automated teller machine. The bank account and the PIN- code are used to get access to the bank account. When using hardware authentication the interaction with the computer is not needed so it doesn´t require any software to work. Hardware tokens usually last for a lifetime so that the user doesn´t have to change batteries or update them anyway. In **Figure 15** an RSA SecurID hardware token is presented. (Pienmunne & Paulow 2009: 33.)

Figure 15. RSA SecurID hardware token (RSA SecurID 2013).

The **Software token** (see **Figure 16**) was made so that the user doesn´t have to carry a separate token hardware. The Token software is flexible and it supports many different kinds of systems. RSA SecurID – software tokens support the same algorithms as RSA SecurID –hardware tokens. Instead of installing the symmetric key to hardware it is now being stored into the mobile phone or PDA. The symmetric keys could also be installed into a smartcard or USB device and being used together with the software tokens (Pienmunne & Paulow 2009: 33.)

Figure 16. Software token on USB stick (RSA SecurID 2013).

Like hardware tokens, **OTP On-demand** authentication is based on two-factor principle. This means that the user receives an OTP and a PIN-code which is allowed to be used once only. OTP can be delivered to the user who has registered into the service either to mobile phone (see **Figure 17**) or to email. For security reasons the laptop or mobile phone where the OTP is sent must also be mentioned in the authentication service. (Pienmunne & Paulow 2009: 35.)

On-demand authentication makes it also possible that a certain user has access to the company´s data for a limited time only. This can be necessary for a company that hires a worker who does the work outside the company for a

certain amount of time. When the worker leaves from the company, the access can be closed permanently. ABB uses OTP On-demand authentication for the consults. (Pienmunne & Paulow 2009: 35.)

Figure 17. OTP On-demand authentication through mobile phone (RSA SecurID 2013).

3.4. Security threats

In literature the terms threat and attack are commonly used to mean more or less the same thing even though there is a difference between these two terms. Threat can be described as a potential violation of security when there is a circumstance, capability, action or event that could breach security and cause harm to the system. The attack for itself is an attempt to evade security services and violate the security of the system. (Stallings 2011: 39). In UWYT there are fewer threats than in BYOD because in BYOD the device is carried home from work. For this reason companies have to know what kind of threats exists, how

dangerous they are and how they can protect their system against them. If the portable device connected to the network is weakly protected and non-updated the most dangerous threats that need to be avoided are the software threats which can do a lot of harm to the company. In the following sections the four most common software threats are explained.

3.4.1. Software Threats

There are four major security threats in BYOD that need to be avoided; phishing, computer viruses, Trojans and buffer-overflows. If the software that the company is using is not updated regularly there can be some serious security threats within them. The best way to reduce the software threats to the minimum is to update when a new version is available. Below in the next chapters the major security threats are explained in more detail.

Phishing is an attempt where some third party people attempt to acquire data like user names or passwords through email or through some faked WWW-addresses. Usually the addresses and pages are quite close to the original thus it is difficult to recognize that it is the wrong website. (Umesh & Bishwa 2012: 2.)

Computer virus is a malicious computer program that can infect several computers. There are also other types of malware such as adware and spyware programs which are created to watch what the user does with his computer. The difference between a true virus and a malware is that a virus can spread

from one computer to another (in a form of executable code) whereas malware and adware doesn´t. Users can spread it over a network or the Internet or even carry it with their USB, disk, CD or even DVD. (Umesh & Bishwa 2012: 1.)

A **Worm** is also a self-replication program which does not need another program in order to be executed. The difference between worm and virus is the way of replication; worms replicate over network connections while viruses replicate on a host computer. (Karresand 2003: 1.)

Trojan horse is a program performing for the user unknown and unwanted actions while at the same time posing as a legitimate program. Some Trojan horses are equaled to a non-replicating virus and other times it is referred to as a super-class to viruses and worms. Even though there is a slight difference between a Trojan horse, worm and a typical virus.. Below in **Table 2** you can clearly see that even the anti-virus vendors (Symantec, Trend-Micro, eEye, F-Secure) could not distinguish between a Trojan horse, worm or a virus. (Karresand 2003: 1.)

Table 2. Example categorization of worms according to four anti-virus vendors. (Karresand 2003: 2.)

Software weapon name	F-Secure	Symantec	Trend Micro	eEye
CodeRed	Worm	Worm	Trojan and worm	Worm
CodeRed II	Worm	Trojan and worm	Worm	Worm
Nimda	Virus and worm	Virus and mass mailing worm	File infector and worm	N/A
Sircam	Mass mailing worm	Mass mailing worm	Worm	N/A

Web bug is a script (usually a java object) which is embedded into a web page. When you visit that particular website, it will be installed on your system. It is usually invisible for the user so it can make some damage to the computer without recognizing it. (Umesh & Bishwa 2012: 2.)

3.4.2. Risk Analysis

The most common response when a computer security professional tries to secure enterprise and desktop to employee is that "I don´t have anything on my computer a hacker would want." That is mostly true because usually the hacker´s aren´t interested about the data on the computer they hack. Instead they want to use the computer for attacking other computers. For the distributed denial-of-service (DDOS) attack the hacker needs many computers connected to each other and one way to achieve this is to take control someone´s home computers. For ABB it is very important to create a risk analysis document which will include all the possible risks that BYOD can create. Along with software threats there are also humans (employees, third persons), hardware's, net (firewall) and authentications that can cause a threat to the company. These risk factors can be divided into four different groups (hardware, human, net and authentication) and they will be explained briefly within the next four chapters.

Hardware is always a risk to the company. Radiation is one of the risk factors that are mostly underestimated. Graphics card and CRT (Cathode Ray Tube) always have a small radiation that can be absorbed with special receivers.

Another risk factor is wiretapping of weak shielded hardware and an uncontrolled entrance to the server and working place. Because the laptop is on the move more than a job PC there is always a risk that a third party could wiretap your hardware and get access to your data. It is also possible that when someone leaves the laptop or mobile phone for a moment alone someone could come and reset the BIOS (Basic Input Output System) settings by clearing the CMOS (Complementary Metal Oxide Semiconductor) where the settings of BIOS are stored. After that the person could get data stored to the computer by using a Linux live CD.

The other workers as well as third party people are always a risk factor in companies. If too many user rights are given the employees could do some harm to the system. It is important that the employee is educated enough to protect himself against the security threats.

The third risk factor is the net. An unprotected network is like an open door to the company. It´s very important to have a good firewall and virus protection to get protected against different attacks and viruses.

The fourth risk factor and one that needs to be carefully thought is the authentication of the workers. It is necessary to use secure passwords containing big letters, small letters and at least numbers to make them secure enough against hackers. The company should also monitor and limit the user

rights so that the user isn´t allowed accessing another department's information through their software, for example.

3.5. Information Security and compliance

When a company becomes global and operates in many different countries the harder it becomes for it to maintain a high security level within its system. ABB has its own information security department locally which follows its users and the programs they are using. There are many different security issues that need to be taken into consideration while creating a strong security system for BYOD and they are discussed in the next section.

3.5.1. Security considerations

The users who accept the BYOD policy in ABB can work at home or at work with their devices. Thus it is really important for the employees to have a secure connection when they connect to the corporate network. The network connection must be handled through a secure VPN (Virtual Private Network) which makes the connection more secure. ABB uses IPSec protocol for the VPN authentication.

The application control is also important for the company perspective because if the employee installs software that is harmful for the system it can cause

serious troubles. Because of the Finnish national laws it is not allowed to check what programs the employees are using, a BYOD agreement must be made. This agreement contains a list of programs that are allowed to be installed.

Since several different IOS (Android, Windows 8 RT and Mac OS) are used among the BYOD test users unique solutions must be made for each operating system when it comes to VPN and security solutions. To protect the IOS against viruses and malwares good and regularly updated antivirus software is needed. For Windows RT operating system it isn´t possible to install any software outside from the Windows store and that demands the Windows RT user to use the antivirus software that Windows provides. Because in the past ABB has used only Windows –based computers and laptops, most of the contracts related to security issues have been made for Windows. That is why for example in Mac OS ABB had free hands to choose what antivirus software is most suitable and best for the company. Because the BYOD is still in pilot mode it was decided to use ClamXav which is free antivirus software under the GNU open source software license. For Android devices ABB also had free hands, so after going through several options from the Android market, Android Antivirus was chosen for the pilot BYOD test.

USB drives, MP3 players, CDs, DVDs and other removable media can pose a real threat to any device (see **Figure 18**). For example network worms can take advantage of USB and other types of removable drives and even PDF files can hide a web-based attack inside them. Application control can be used to block attacks from removable drives and even preventing some programs to write

code to a machine (Symantec 2013). For device control Symantec, Check Point and McAfee are the most well-known service providers world-wide. In ABB the device control has been handled by McAfee for Windows operating systems but because of the time limitations for the thesis it was decided that it won´t be installed on Android, Mac OS or Windows RT at all. For Windows RT it would have been impossible to install because it can't be found in the app store.

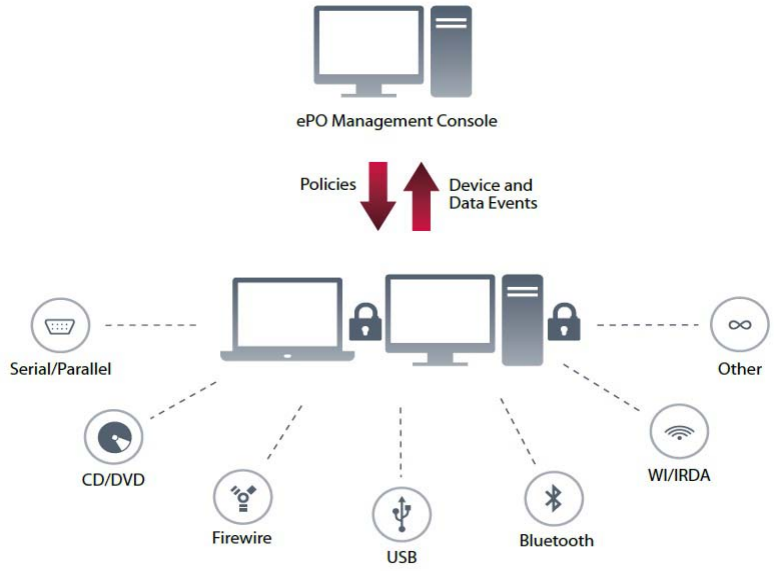

Figure 18. List of devices controlled by device controller (McAfee 2012).

3.5.2. Compliance considerations

There are several different important compliance considerations that need to be solved before the employee can start using the BYOD device. First and foremost the end user agreement must be made among the employee and ABB and it must contain the list of rights the employee has and list of rights what the employer has. Before signing the user agreement the employee needs to go

through it and must understand the details of the agreement fully before signing it. For example if the laptop containing ABB data gets stolen or lost, ABB must have the permission to wipe-out the computer after certain amount of time if the computer can´t be found. The employee must know the risks of saving data on the computer without having a back-up. Another important issue related to the user rights are the programs that can be installed on the device. Apple and Windows RT have handled it well because it is controlling its own application store but for Android the store isn´t controlled so well so the employee must be aware of the risks that might come when he downloads the software online. Because the device is owned by the employee he is allowed to install the software he needs from the store but must be aware of the risks of an infected application.

A further issue is the licensing that plays an essential role when a device is owned by both company and the employee. There is several different software that are free to download for private usage but for business you have to buy a license. The question in this case is, if the software requires a license or not? At the moment it is not regulated by the law.

Security awareness is also one of the key elements in creating a successful BYOD system. Within the company the software is automatically updated and maintained by the IT support but in BYOD the employee itself must be aware of the recent updates and risks about the recent trends in internet security. The company is responsible of giving the employees enough information about the risks as well as training them to become more well-known about the security of

their working devices. The software must be updated automatically so that the computer always has the latest and most secure versions of the software.

4. INTERNET OPERATING SYSTEMS IN BUSINESS WORLD

There are several different IOS (Internet Operating Systems) that are used in the business world today. Ten years ago most of the companies used only Windows as their main Internet operating system. The rapid growth of mobility has brought a lot of different other operating systems. These can be divided into three categories. To the first category belong operating systems, that the mobile company has created themselves. Examples for this category are Apple iOS, RIM´s BlackBerry OS and HP´s WebOS which was previously known as PalmOS.

To the second category belong operating systems where a developer has developed an operating system that can be installed in different mobile phones, but the OS developer doesn´t manufacture phones themselves. The best example for this category is Windows 7 which can be used in any mobile phone but the company isn´t manufacturing any mobile phones.

In the third category there are operating systems which are based on open source codes. Examples for this group are Meego, Android and Symbian. Anyone can use these open source operating systems in their own devices and edit them the way they want to. (Avikainen 2012: 21.)

4.1. Windows (PC)

Windows is the most commonly used operating system in today's world. According to W3schools (2013) the operating systems from the Windows family are installed on 82,5% of the computers in 2013. 55% of the devices today are using Windows 7 which means that Windows 7 is the most common operating system today. (Avikainen 2012: 21.)

The latest version of Windows is 8 which was launched on October 26th, 2012. At the same time when Microsoft launched Windows 8 it also launched their first operating system for tablets, Windows RT. The Windows RT user interface (UI) is same than in Windows 8 and they also share some same code, but they are still distinct operating systems designed for different classes of devices and run on different processors. Windows 8 runs on Intel´s x86/64 processor architecture, Windows RT only works on devices with ARM (Advanced RISC Machines) -licensed CPUs (Central Processing Unit). While Windows RT lacks certain features and compatibility in comparison to Windows 8, Microsoft aimed for Windows RT devices to take advantage of the ARM platform's power efficiency (allowing for longer battery life) and to support system-on-chips which allow a thinner hardware designs. Microsoft also focuses on the new Windows Store platform for touch-optimized apps to provide a reliable OS which is easy to use for their customers. The only desktop applications officially supported by Windows RT are those that come with the operating system itself (such as File Explorer, Internet Explorer, and the Office RT programs). Only Windows Store applications (which use WinRT, a new cross-platform application architecture that is processor instruction set independent and

supports both Windows 8 and RT) can be installed by users on Windows RT devices (Keizer 2012: 1). This causes problems for many businesses because they use certain software for certain services like emails (Lotus Notes in ABB Finland).

4.2. Linux

Linux is an operating system started by a Finn called Linus Torvalds in 1991. Linux is a free operating system and the source code to it can be found online. It was an early alternative to other UNIX workstations offered by Sun Microsystems and IBM. Today Linux is a full-featured UNIX system that runs on many platforms including Intel Pentium and Itanium as well as in Motorola/IBM PowerPC. (Stallings 2008: 94.)

4.3. Apple Mac OS

Apple Mac OS is a graphical user interface –based operating system that has been developed by Apple Inc. for their Macintosh computers. The first version of the Mac operating system was introduced in 1984 with the original Macintosh. The latest stable version of this operating system is 10.8.2 (Mountain Lion) which was released in November 2012.

4.4. Windows Phone 8

Windows Phone 8 is the latest mobile operating system in windows mobile phones. It has been available to consumers since the 29th of October 2012. It is programmed in C / C++ and runs with devices like Nokia Lumia 920 –mobile phone. User interface of Windows Phone 8 can be seen from **Figure 19**.

Figure 19. Windows Phone 8 user interface (Jain 2012).

4.5. Android

Android is a quite new operating system for mobile devices. Google bought Android Inc. in 2005 and started developing their own Android platform. Android is a Linux-based operating system which is designed primarily for

touchscreen mobile devices such as smartphones and tablet computers. It is the world´s most used smartphone platform (Avikainen 2012: 21). From **Table 3** can be seen the different versions of Android and their current distribution among Android users. (Android Developers 2013.)

Table 3. Distribution and different versions of Android (Android Developers 2013).

Version	Codename	API	Distribution
1.6	Donut	4	0.2%
2.1	Eclair	7	2.2%
2.2	Froyo	8	8.1%
2.3 - 2.3.2	Gingerbread	9	0.2%
2.3.3 - 2.3.7		10	45.4%
3.1	Honeycomb	12	0.3%
3.2		13	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	29.0%
4.1	Jelly Bean	16	12.2%
4.2		17	1.4%

4.6. Apple iOS

Apple is known for having its source code private and it sometimes makes things more complicated when connecting Apple device to some other system. The first version of iOS was released in 2007 for iPhone and iPod Touch. It has been developed for the touch screens and it differs a bit from the Mac OS X. The latest version of Apple iOS is 6 which was released in September 2012 (Costello 2012).

5. BYOD SECURITY SOLUTION FOR ABB

This chapter of the thesis contains confidential information about the BYOD security solution for ABB as well as personal interviews about the ABB BYOD pilot. It is removed from the public and remains secret.

6. CONCLUSION

Bring Your Own Device (BYOD) is a technology that is here to stay. When allowing employees to use BYOD the companies are opening a new chapter for security managers and administrators. The security governance framework and corporate security policies will need to be redefined and a great deal of effort will be required to make each policy efficiently operational and streamlined. Even more and more companies have started to allow their employees to bring own devices to working place and use them for accessing the corporate network and personal work-related software. There are several different Internet operating systems, with different strengths and weaknesses which made the creation of BYOD complicated for ABB. The company has a really strict security policy which didn´t allow to use one solution for all the operating systems but instead an own solution for each system was required. Since the IT departments are located in different countries it took quite much time before all the devices had access to a corporate network and before all the software required for security was installed.

Even though BYOD is already in use in different companies there is still a lot of future work and questions that need to get answers before it can be fully applied to everywhere. For the future work the main questions about creating a successful BYOD policy to ABB is to find answers to software license related issues which haven´t been solved in any companies in Finland so far. Is it allowed for the employees to install personal software to their own working device without buying the business license to it? Who can tell if the person uses the software for business usage or personal usage? It is a question that most

likely first needs a lawsuit and solution before it can be fully answered. Another question that needs to be considered is that what happens to the company data when an employee suddenly decides to change a job and leave the company? Will the computer be wiped out of data or will the employee just remove all the company software?

In this pilot phase only four people got the BYOD device for test use and it took a lot of time to create a system that is secure for the employees. The devices and settings were set up by professionals so a big question that will remain is that will the employees be able to set up their own devices by themselves or do they need help setting them up? If the BYOD policy will be applied to a larger amount of people the set up should be so easy that almost everyone could do it successfully when following the instructions step by step. When connecting to the corporate network the BYOD device must be tested somehow to make sure that it contains all the latest required software updates and patches to make the connection as secure as possible. A good suggestion to this question and maybe a future work would be to create a test system that tests the BYOD device´s installed software and makes sure before allowing the connection that the device is up to date.

For the future work it would be good to do a system and software scan for the BYOD device before it is allowed to connect to the corporate network or service cloud to make sure that the software is up to date. The BYOD device would also need to have a strong passcode for login and full-disk encryption for disk, removable media and cloud storage to keep the system as secure as possible.

For BYOD in ABB the best and most secure way to operate would be a well-protected service cloud which would be compatible with different operating systems. This would make the BYOD more secure in ABB when everything goes through a secure service cloud and the device connecting to the cloud is scanned before it connects to it. For mobile phones a Mobile device management (MDM) would be vital to delete the sensitive company data if the device gets stolen or lost. Also for both laptops and mobile phones a proper application control would be essential to make sure there isn´t any suspicious software running while connecting to the company´s service cloud.

There is demand for BYOD in ABB like there is in many other big companies around the world but only the future will show how big the BYOD trend will eventually become and will it replace the old way of thinking permanently.

REFERENCES

ABB Group presentation February 2013. ABB Intranet 2013.

Android Developers 2013 [online]. Available from the Internet: <URL: http://developer.android.com/about/dashboards/index.html>. Read 5.3.2013

Aqun, Zhao, Yuan Yuan, Ji Yi & Guangun Gu. (2000). Research on tunneling techniques in virtual private networks. Digital Object Identifier: 10.1109/ICCT.2000.889294

Avikainen, Sari (2012). *Muuttuvan laitekannan hallinta – BYOD ja tietotekniikan kuluttajistuminen media-alan yrityksessä*. Opinnäytetyö. Haaga-Helia University of Applied Sciences.

Butler, Shawn A (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach [online]. Available from the Internet: <URL: http://www.cs.cmu.edu/~shawnb/SAEM-ICSE2002.pdf>.

Butler, Shawn A (2003). Security Attribute Evaluation Method [online]. Available from the Internet: <URL: http://reports-archive.adm.cs.cmu.edu/anon/anon/usr0/ftp/usr/ftp/2003/CMU-CS-03-132.pdf>.

Burt, Jeffrey (2011). BYOD Trend Pressures Corporate Networks [online]. Available from the Internet: <URL: http://winfwiki.wi-fom.de/images /2/2e/65469365.pdf/>.

Costello, Sam (2012). iPhone Firmware & iOS History [online]. Available from the Internet: <URL: http://ipod.about.com/od/iphonesoftwareterms/a/ firmw_history.htm/ >.

Egan, Matt (2013). Do Apple Macs need antivirus? OS X security explained [online]. Available from the Internet: <URL: http://www.pcadvisor.co.uk/ features/security/3418367/do-apple-macs-need-antivirus-os-x-security-explained >.

Ellis, L. , Saret, J. & Weed, P. (2012). BYOD: From company-issued to employee-owned devices. Telecom, Media & High Tech Extranet 2013.

Huuhka, Riku (2011). Turvallisen Etäyhteyden Luominen. [online]. Available from the Internet: <URL: http://publications.theseus.fi/bitstream/ handle/10024/24740/Huuhka_Riku.pdf?sequence=1>. Opinnäytetyö. Oulu University of Applied Sciences.

Innanen, Heikki (2003). VPN Virtual Private Network [online]. Available from the Internet: <URL: http://www2.it.lut.fi/kurssit/02-03/010626000/ palautukset/seminaarit/vpn.pdf/ >.

ISF Grey Chapter Meeting ZRH (2012). Bring Your Own Device – A Challenge And An Opportunity.

Jain, Pragati Chaplot (2012). BYOD: Nuisance or Need? [online]. Available from the Internet: <URL: http://www.maas360.com/maasters/blog/mobile-device-management/byod-nuisance-or-need/ >.

Kapoor, Vivek, Sonny Abraham Vivek & Ramesh Singh (2008). Elliptic Curve Cryptography. ACM Ubiquity, Volume 9, Issue 20. <URL: http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/abhishek3.pdf/ >.

Karresand, Martin (2003). Separating Trojan Horses, Viruses, and Worms - A Proposed Taxonomy of Software Weapons. ISBN 0-7803-7808-3/03/$17.00 @ 2003 IEEE

Keizer, Gregg (2012). FAQ: All about Windows RT, the OS behind a Microsoft tablet [online]. Available from the Internet: <URL: http://www.computerworld.com/s/article/9228202/FAQ_All_about_Windows_RT_the_OS_behind_a_Microsoft_tablet/ >.

Lifehacker (2013). How to Make Your VPN Even More Secure [online]. Available from the Internet: <URL: http://lifehacker.com/5902397/how-to-make-vpns-even-more-secure/ >.

Miller, Keith, Jeffrey Voas & George Hurlburt (2012). BYOD: Security and Privacy Considerations. 1520-9202/12/$31.00 ©2012 IEEE

Ortiz, Sixto (1997). Virtual private networks: leveraging the Internet. Digital Object Identifier: 10.1109/2.634834.

Pienmunne, Juhamatti & Jari Paulow (2009). *Kertakäyttöiset salasanat tietoverkoissa*. Opinnäytetyö. Kymenlaakso University of Applied Sciences.

Priyadarshi, Gaurav (2013). Leveraging and Securing the Bring Your Own Device and Technology Approach. ISACA Journal Volume 4, 2013 (Language Of Cybersecurity).

Ramsey, Matthew (2013). State Of Cloud Computing [online]. Available from the Internet: <URL: http://www.business2community.com/tech-gadgets/state-of-cloud-computing-0381119/ >.

Rounak, Jain (2012). First Update to Windows Phone 8 Apollo Might Be Called Portico, Not Apollo+ [online]. Available from the Internet: <URL: http://androsym.com/news/first-update-to-windows-phone-8-apollo-might-be-called-portico-not-apollo/ >.

Salmio, Petri (2012). *Pilvipalvelut*. Opinnäytetyö. Turku University of Applied Sciences.

Sanouvong, Tim (2013). BYOD – An Emerging Technology Concept [online]. Available from the Internet: <URL: http://www.blogs.oracle.com/OracleIDM/entry/partner_blog_series_deloitte_talks />.

Shaikh, F.B. & Haider, S. (2011). Security Threats in Cloud Computing. 978-1-908320-00-1/11/$26.00 ©2011 IEEE

Singh, Niharika (2012). B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel" ISSN No: 2319-5614

Stallings, William & Lawrie, Brown (2008). *Computer Security – Principles and Practice.* Pearson International Edition. Pearson Education Inc. ISBN 0-13-513711-X

Stallings, William (2011). *Cryptography and Network Security Principles and Practise.* Fifth Edition. Pearson Education Inc. ISBN 0-13-705-632-X

Stallings, William (2008). *Operating Systems: Internals and Design Principles*. Sixth Edition. ISBN-13: 978-0-13-600632-9

Symantec (2013). Security Response [online]. Available from the Internet: <URL: http://www.symantec.com/security_response/securityupdates/list.jsp?fid=adc/ >

Symantec (2013). Internet Security Threat Report 2013 [online]. Available from the Internet: <URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf >.

Trend Micro (2012). TrendLabs2012 Mobile Threat and Security Roundup [online]. Available from the Internet: <URL: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf >

Torro, Tuomas (2007). *VPN-ratkaisujen vertailu*. [online]. Available from the Internet: <URL: http://www.doria.fi/bitstream/handle/10024/28149/stadia-1192088317-3.pdf> Insinöörityö. Helsinki Metropolia University of Applied Sciences.

Umesh, H. & Bishwa, Pati (2012). Study Of Internet Security Threats Among Home Users. 978-1-4673-4794-5/12/$31.00 @2012 IEEE

W3schools, 2013. OS Platform Statistics [online]. Available from the Internet: <URL: http://www.w3schools.com/browsers/browsers_os.asp/> Read: 04.03.2013.