TALLINN UNIVERSITY OF TECHNOLOGY

Interactive Cyber Security Awareness Program

Master Thesis

Predrag Tasevski - 106937IVCMM - ITI70LT

Tallinn, 2012

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology
Department of Computer Science
Chair of Network Software

Supervisor
Dipl. Eng. Jüri Kivimaa

Date of the graduation
11 June 2012

“The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.” Sun Tzu (Chinese general and author, b.500 BC)

Contents

Autorideklaratsioon

Deklareerin, et käesolev lõputöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud.

....

(kuupäev) (lõputöö kaitsja allkiri)

Abstract

Currently, humans coupled with the socio-technical aspect can be either the strongest or the weakest link in any information security system, and the key in security lies in delivering awareness training through short and effective online videos, whereby the participator can gain knowledge on security. Our aim, therefore, is to develop innovative solutions to deliver an interactive cyber security awareness program, where the main goal is to enhance information on security awareness and knowledge in organizations, schools, nations, homes etc. The syllabus consists of a systematic approach divided into three sections. The introduction is a basic level course (BASIC), with the aim of delivering an elementary curriculum in physical security, computer and mobile; network and Internet security to everyone. It is made up of several units with interactive training videos that last less than 10 minutes each. The second course (ADVANCE) is the advanced program which demonstrates the attacking phases, different attacking methods and the countermeasures that highlight the anatomy of Advance Persistence Threats (APT). This curriculum is intended for administrators, help desk personnel, information technology professionals among others. The last course (MANAGEMENT) is intended for managers, where we annotate two decision-making processes with their cycle loop. Moreover, after each unit there is a questionnaire, which measures the knowledge of each participant, and compares it to the base-line survey carried out during the registration process. As a result, it represents the participant's awareness level and knowledge, and will assist in further actions if necessary. By implementing this program in private and public organizations, governments, schools and universities will lead to the improvement of security in the everyday use of computers, mobile phones, online banking, social networking_ both at home and in the workplace. The present study addresses and implements the IT security issue. We will apply the results by carrying out the syllabus, with the latest improvements, in universities and private organizations. Consequently by applying these further improvements to the syllabus, it will meet the needs of the cyber security field.

Abstraktne

Praegu võivad olla mistahes infoturbe süsteemi kõige tugevamaks või nõrgemaks lüliks inimesed koos nende sotsiaal-tehnilise aspektiga. Võti turbe suurendamiseks seisneb kasutaja teadlikkuse tõstmises läbi efektsete veebipõhiste lühivideode. Selletõttu on meie eesmärk arendada innovatiivseid lahendusi interaktiivse küberkaitse programmi jaoks, mille peamine ülesanne on tõsta infoturbe alast teadlikkust organisatsioonides, koolides, kodudes ja mujal. Õppeplaan koosneb süstemaatilisest lähenemisviisist, mis on jagatud kolme osasse. Sissejuhatus on algtasemeline kursus (BASIC), mille eesmärk on läbi viia lihtne õppekava füüsilise, arvutite, mobiiltelefonide, võrgu ning Interneti turbe teemal. Koostatud on see mitmest erinevast osast, milles igaühes on alla kümne minutilised interaktiivsed õppevideod. Teise kursuse puhul (ADVANCE) on tegemist edasijõudnud programmiga, mis demonstreerib rünnaku faase, erinevaid ründe meetodeid ning vastumeetmeid, mis tõstavad esile püsivaid sihitud ründe ohte (APT). See õppekava on mõeldud administraatoritele, help desk'i personalile ning teiste hulgas ka infotehnologia professionaalidele. Viimane kursus (MANAGEMENT) on suunatud juhtidele, selles võetakse kokku kaks otsustavat protsessi koos nende elutsükliga. Lisaks on iga kursuse osa lõpus küsimustik, mis mõõdab kõigi osalejate teadmisi ning võrdleb neid registreerimise protsessis läbi viidud baasuuringuga. Lõpptulemusena näitab see osalejate teadlikkuse taset ja teadmisi ning vajadusel abistab neid nende tulevastes tegevustes. Antud programmi rakendamine era- ning avalikes asutustes, valitsustes, koolides ja ülikoolides edendab turvet igapäevasel arvutite, mobiiltelefonide, internetipanganduse ja sotsiaalvõrgustike kasutamisel nii kodus kui töökohas. Käesolev uurimus pöörab tähelepanu IT turbe teemale. Me rakendame tulemusi õppeplaani ning uusimate täiendustega viime seda läbi ülikoolides ning eraasutustes. Lisades edasisi uuendusi õppeplaani, vastab see küberkaitse ala nõuetele.

1 Introduction

Since the beginning of writing, leaders of nations and the military understood that it was necessary to yield mechanisms that could protect the confidentiality of written correspondence and to have the means of detecting tampering. Hence, Julius Caesar invented the Caesar cipher to communicate with his army by the employment of encryption for the sake of securing messages [49]. Furthermore, World War II saw the use of an Enigma machine by German military field agents to encrypt and decrypt messages and communications[1]. The end of the 20th century and the early years of the 21st century have seen a rapid growth in telecommunications, the production of simultaneous computer hardware, and consequently software, etc. Computers quickly became interconnected through a network which is today known as the *Internet*. The vertical growth and widespread use in everyday duties of technology through the Internet has led to numerous professional organizations, academic disciplines of computer security, information security and information assurance invoking a definition of information security. The main goal of *information security* is to protect information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Hence the preservation of the confidentiality, integrity and availability of information [3]. Likewise *cyber security* is protecting Information and Communication Technologies (ICT) systems and Critical Infrastructure (CI) [64].

Nowadays, businesses, organizations and citizens find ICT invaluable for carrying out daily tasks both at home and in the workplace. Analogous to the greater population, organizations and businesses are likely to suffer from security breaches. This is due to vulnerabilities in the new and existing technologies together with device convergence. Such security breaches may be IT related, for instance, through computer viruses or malicious software, data corruption or system failure, or may be as a result of social motivation, for example, incidents caused by human factors. Recent stories have highlighted that a considerable number of end-users are unaware of their exposure to security risk. Through breaches seen recently, it is more critical than ever that organizations raise security awareness by turning users into a first line of defence [41].

However, the most important protection element in IT security is to reduce business risk to accepted levels and the protection of entire information and information systems essential to the organization. Alternatively cyber security aims at assuring

[1] 1937 Enigma Manual by: Jasper Rosal - English Translation [32]

critical IT services for CI and CII on accepted levels, in addition to the protection of critical information / information systems of national CI (i.e. protection of national CII). In other words the security objective determiner in information security is an organization's business process, while in cyber security it is for the entire state. Emphasizing that states may have different or complementary interests compared to an organization's business interests. On one hand, handling cyber security problems is considered to be both a nationally and internationally coordinated activity to protect national CII. On the other hand, handling information security is mainly an institutional level activity, utilized only for specific institutions / situations nationally and legislatively managed by the state. Similarly, to information security objectives: confidentiality, availability and integrity, in cyber security the additional objectives are non-repudiation, authentication, information systems importance and criticality from the standpoint of state CII/CI.

Furthermore, in the case of cyber attacks and/or cyber warfare into the social sphere, cyber security takes into account: human behaviour, the flow of information in a crisis situation and social networks, while this information is normally not considered in information security. Another point in the action plans for a cyber crisis is that IT security involves Business Continuity Plans and IT recovery plans, whereas in cyber security significantly higher level action plans are required to ensure CI processes continuity and the necessary CII recovery.

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and to respond accordingly [66]. IT security awareness programs are common approaches or models necessary to centralize policy, strategy, implementation and also to distribute the implementation and strategy for a certain, specific organization by improving the information systems in security through implementation of new assets. Moreover, the weakest links can also lie in technologies, implementation of technology and software. Cyber security awareness programs are composed of IT security, the flow of information in a crisis, plus the social sphere, for instance social engineering, the human element and social networking. In cyber security the implementation is designed for all organizations, an element that is included into CI/CII at a national level. The priorities in cyber security awareness programs are to raise the knowledge, and to develop a strategy at the nation level, IT security awareness also reflects the organizations strategy for complying to its awareness standards and responsibilities.

Therefore, in this paper the main goal is to embrace awareness at a national level of the weakest element in security by providing a syllabus. The program concerns different target groups and defines the communications concept. Effective communication planning is critical for the program's success. Additionally, it defines the goals and objectives of the program. Consequently, it defines the indicator to measure the success of the program and focuses on delivering "*best practices*". Evaluation and feedback mechanisms are critical components of any security awareness program. Thus baseline surveys of the current status are taken beforehand and aim to track the benefits brought about by the awareness programme. Evaluation questionnaires were used to solicit feedback from the respondents.

However, the security landscape is continually changing the advancement and proliferation of security threats, the cyber security solutions of today will be obsolete tomorrow. Most analysts report that the human element of any cyber security framework is the weakest link. Thus, a lack of awareness among staff, reduces the strength of the first line of defence [61]. Therefore, only a significant change in user perception or culture can effectively reduce the number of information and cyber security breaches.

This following chapter illustrates the problem statement of the thesis. It deals with the activities of related work and closes with an outline of the paper.

1.1 The Problem Statement

Although organizations are implementing the strongest cyber security systems, they cannot provide fully effective protection against all cyber attacks. The issue is not because they are inadequate, but because many aspects of current systems rely on the users and their decisions. This is known as the human factor. Humans are the weakest link when it comes to cyber security. The latest reported breaches were caused by unintentional mistakes made by the employees and the majority of the breaches could have been avoided if some of the most common mistakes had not been made. Having pinpointed the problem, action needs to be taken, by implementing educational training programs whose main aim is to boost and improve the awareness knowledge. If the employees dedicate a few minutes from every day work tasks to improve their knowledge in security this will aid in the protection against cyber attacks and threats to organizations. Additionally, best practice shows that delivering training through short videos to the employees is a more convenient way than delivering training through presentations, the classroom approach, etc. The awareness program should be available and accessible to everyone. The idea is not only to implement the knowledge in organizations, but also in home usage of technology. For example, many employees nowadays connect to the company network through moveable devices, for instance, mobile phones, tablets PC, company or personal laptop, notebook, etc. All the above grant the attackers an easy way to bypass the first line system guard.

Currently, many organizations, schools and nations are implementing different approaches to increase the level of awareness. One approach is to issue a guide to provide practical and effective advice to private organizations and the public at large, allowing the reader to prepare and implement information security awareness initiatives that apply to them [41]. For instance, non-governmental organizations (NGO's) are addressing the issue that further development of cyber security awareness programs should be implemented. For example, ENISA - European Network and Information Security Agency [41] has developed a users' guide: "How to raise information security awareness", where they provide practical advice for member states to prepare and then implement awareness raising initiatives related to information security. Moreover, NIST - National Institute of Standards and Technology [66] publish detailed guidance on designing, developing, implementing, and maintaining an awareness and training program within an agency's IT security program. In addition, SANS InfoSec Reading Room[2] developed a Security awareness program too. Alternatively, the University of Arizona[3] developed a security awareness site that contains awareness presentations, videos and posters. The program delivers training for all employees, training for users with elevated privileges and additionally for web developer's education and awareness program. IWS [4] is another online resource that aims to stimulate debate on a variety of issues involving information security, information operations, computer network operations, homeland security and more. Furthermore, they provide you with a Security Awareness Toolbox[5] and an Information Systems Security Awareness course[6]. Further examples are highlighted in the related work section.

However, there are enormous differences between each awareness program. Up to now almost all the academic effort in information security training has concentrated on solving the technical and policy aspects of the problem rather than designing security systems and mechanisms to take into account the human factor which is thus resulting as the most vulnerable element to the threats in systems. This jeopardizes the overall efficiency of the organization and nation.

Nevertheless, new proposals may surpass the actual style of delivering security awareness programs. Lance Spitzner [54], discusses why humans are bad at judging risk, where he points out the problems when humans interact with technology. Firstly, people feel like they are in control. They decide which websites they visit, the e-mail they read, and the links they click on, which applications to install or which films or music to purchase. Since people have a sense of control, they underestimate risks on the Internet. In most cases, people never know their system is hacked. Nothing visual or catastrophic happens on the screen; hence once again people often downplay or underestimate the risks. Secondly, unlike the physical word, in cyber space you cannot see who you are communicating to. As a result it has become very simple for attackers to pretend to be individuals or organizations that people trust. Therefore, Lance Spitzner shares his ideas on how to create a successful security awareness program, where the goal is to change people's understanding of these

[2] SANS InfoSec: `http://www.sans.org/reading_room/whitepapers/awareness/`, last checked 17.04.2012

[3] University of Arizona: `http://security.arizona.edu/basics`, last checked 17.04.2012

[4] IWS - The Information war fare site: `http://www.iwar.org.uk/index.htm`, last checked 17.04.2012

[5] Security Awareness Toolbox: `http://www.iwar.org.uk/comsec/resources/sa-tools/`, last checked 17.04.2012

[6] Information System Security Awareness course: `http://www.iwar.org.uk/comsec/resources/awareness/index.html`, last checked 17.04.2012

risks, and ultimately change their behaviour. The key to having an awareness program that creates a secure environment is answering these three questions: Who? What? How?

- *Who?* determines the target of your awareness program.
- *What?* determines the content of what to deliver and teach people.
- *How?* is the means by which you communicate content.

Next, many awareness programs are outdated and use traditional learning methods, for instance: presentation, discussion group, training, etc. The difference is in approach, what may have worked for employees 30 years ago, no longer works for the YouTube generation. Most people now communicate in short sound bites. Spitzner remarks that one of the most effective methods for delivering an awareness program is through short videos, online communication that grabs a person's attention, videos they want to watch and learn from.

The purpose of our work is to develop an online environment that includes a set of best practice, hands-on and with a management plan focus by demonstrating the attacking phases and the different attacking methods, and finally showing how to bypass an attack. Our aim is to identify proposals for future improvement as well and to create our own course management system suitable for survey, questionnaire and training purposes. We determine the answers to the above three questions. The target groups for delivering the awareness program are: basic, advance and management. We determine the content of what to deliver and teach. Additionally communication is done through short online videos, of no more than 10 minutes. A baseline survey is distributed to the participants beforehand to measure their prior knowledge, and after the completion of the the course the results will be examined and the similarities and/or differences will be noted.

1.2 Related Work

Despite the various amounts of awareness programs, their approaches and methods are different. The ideas for the awareness program we have implemented are usually not new, but the uniqueness of our awareness program lies in the style of communication, the systematical approach of the targeted groups and the content delivered. Consequently, the uniqueness of our program lies in the communication, course content, management system, systematic approach of the scoreboard, the discussion board, tests, the different levels to which this course is applicable, for example, the different targeted groups: basic, advance and management. Also the baseline survey is unique, because it is applied afterwards and compared to the questionnaire quiz, and in the end the topic advisor which helps the participants and users gives advice related to their knowledge.

Cyber security and information security has been applied at several universities as a master's degree program, like the Tallinn Technical University (TTÜ) master studies of Cyber Security, the University of Oxford offers Software and System Security[7], for the sake of securing the university campus. Additionally, an enormous amount of programs have been developed by different types of organizations, either state organizations or NGO. The approaches seen up to now are usually either in written form, or in cyber security awareness campaigns such as, the comic strip from Sémafor Conseil SA[8], a video campaign from the University of Tennessee[9] or campus security awareness like the one from the University of Arizona[10]. Another approach is by delivering interactive videos, for instance, SANS Securing the Human[11] or IASE Education, Training and Awareness[12]. Alternatively, private companies are providing different types of training or awareness programs, such as eLearnsecurity[13] by delivering penetration testing and virtual laboratory training and many others.

Nevertheless, all of those listed above and many others have different views and approaches to delivering awareness programs. Few of them, have been developed within the demonstration of awareness through short videos, furthermore, none of them have implied the questionnaire quiz techniques, and to measure the prior baseline knowledge before the participants enrolled in the program. Different from the survey and quiz, none of them have developed a topic advisor / mentor for a follow-up action. Other approaches tent to, group or divide the targeted groups, whereby several programs deliver the same topic more or less to the audience, where they have not divided them into specific targets such as, for advance users, or managers. Indeed every manager is a user, but every user can not be a manager.

Furthermore, the courses done in the cyber security master degree program in TTÜ have delivered a wide range of topics. Consider the course “Information Systems Hacking Attacks and Defence” delivers advance methods of hacking attacks through an extremely interesting and valuable scoreboard where the students have to perform real live scenarios, attacks and gain points by answering the questions. With this course in mind, the advance curriculum course of this paper has been developed. We have emphasized the attacking phases firstly and then pursued into more depth details of attacking methods and techniques of countermeasures.

Alternatively, in regard to the advance course, we have not seen current awareness programs that pursue the importance of delivering an awareness programs for managers or dividing the awareness program for everyday users. In fact, many of the approaches are just developed in general way, by illustrating the threats and the countermeasure of bypassing those threats. On the contrary, through our novel

[7] System Security: http://www.cs.ox.ac.uk/softeng/security/, last checked 17.04.2012

[8] Sémafor Conseil SA: http://semafor-conseil.ch/Semafor_Conseil_maitrise_des_risques_et_securite_des_systemes_dinformation_-_securite_reseaux_-_audit_securite/Security_awareness_by_comic_strip.html, last checked 17.04.2012

[9] University of Tennessee: http://my.tennessee.edu/portal/page?_pageid=40,39533&_dad=portal&_schema=PORTAL, last checked 17.04.2012

[10] University of Arizona: http://security.arizona.edu/basics, last checked 17.04.2012

[11] SANS Securing the Human: http://www.securingthehuman.org/, last checked 17.04.2012

[12] IASE: http://iase.disa.mil/eta/, last checked 17.04.2012

[13] eLearnSecurity: http://www.elearnsecurity.com/, last checked 17.04.2012

systematical approach we have separated the three main threats that could arise through the use of computers in every day work, such as the physical security, computer and mobile security issues, followed by the network and Internet problems. Moreover, especially for managers we have reasonably noted and illustrated the necessary decision making process.

We believe that no other previous related work as mentioned above has used such a systematical approach, methods and targeted specific groups of distributing the awareness program as we have done. Neither have they answered the three important and valuable questions during the creation of security environment awareness program as discussed in the Problem Statement. Anyhow the present related awareness programs have remarkably and successfully helped to define the necessary needed action and determined how to develop and create an effective and productive cyber security awareness syllabus.

1.3 Thesis Outline

This paper is organized as follows. In Chapter 2 we give a current curriculum of the syllabus, separated into three parts: basic, advance and management. Additionally, we provide the curriculum for each course divided into separated chapters, where we present the inside modules and units. Chapter 6 delivers a prototype web solution for a course content management system, which describes user usability, student and administration interface. It emphasizes the scoreboard and the topic advisor, whose aim is to scale the knowledge level. Chapter 7 delivers results of carrying out the syllabus to universities and private organizations with the latest improvements, differences and similarities made by baseline results from the survey, their feedback and suggestions about the program. We provide our conclusion in Chapter 8 and further future work. In the Appendix, we provide the survey questionnaire template, without the correct answers.

2 Syllabus

The program supplies a systematic approach for different groups: basic, advance and management. Each part contains a certain a number of modules, divided into units, which are pursued into separate chapters curriculum. The syllabus is built on what to do and what is to be done for information security to be secure, either the possibility of avoiding or mitigating the security incident. The Basic course delivers three securities phases, such as, physical security; computer and mobile security; and network and Internet security. Secondly, the advance course curriculum supplies the participant with the importance of the attacking phases and is followed by the type of attacks, where in the end we note the anatomy and countermeasures for advanced persistence threats. In contrast, the management curriculum distributes two methods for the four phases of decision making process. Overall, the idea of the syllabus is to help, improve and elevate the awareness level of three different types of groups of information security. We emphasize that the weakest element is human behaviour, followed by the socio-technical aspect. Whatsoever, this syllabus does not cover the legal aspects associated with information security matters.

The approximation of the syllabus is to be carried out in different organizations, businesses, as educational systems, in schools, universities and campuses, etc., The basic course will help and guide everyone in the importance and valuable security measures to be taken into account. Followed by the course for more advanced, or in other words expert users, such as IT departments, programmers, etc. which will yield the understanding and superiority of attacking phases, attacking types and APTs; by delivering and divvying the countermeasures that need to be considered. Finally we target, the decision making process phases for the management department.

Moreover, in order for the program to be extremely intriguing after each unit we supply questionnaire quizzes, where the participant has to provide an answer. Each answer is recorded into the database for further analysis. After submission of the answer there is no possible way to change the record. Therefore, the participant can only answer the questions once. However, in order to be able to give the correct answer at the bottom of each unit we present additional reading material and hints which will help and guide the participant to procure beforehand the most reasonable answer to the questions. Also after the registration process is completed, the participants are redirected to the baseline survey where the main idea is to measure the knowledge in advance, consequently to examine and note the similarities or difference of gained knowledge, for more details of the survey template see the Appendix section.

Additionally, we provide the possibility of a discussion board for sharing the user's experience and thoughts about the modules, units and questions. The discussion board is separated into three sections: suggestions, ideas and questions.

The outline of the chapter is presented by three sections. First is the basic course sections, wherein Chapter 3 discusses the modules and inside units. Secondly is the advance course, followed by Chapter 4 where we deliver the attack phases, types of attacks and APTs. Thirdly is the management course, complied within Chapter 5, distributing the decision process making phases.

2.1 Basic

The Internet has become an integral part of our daily lives and computers are operating within a complex networked environment. Whether you are using a computer connected to the Internet in or out of the office, your home, likewise for entertainment, your computer is a target. Frankly, CISCO says that more mobile devices are present than humans in 2012 [12], thus by communicating and using our mobile, portable devices in everyday basis are targets as well. Additionally, in spite of usage and the growth of mobile devices Checkpoint [46] reports that 71% of companies say mobile devices are causing security issues into their corporate environment. Furthermore, recent research at ENISA states that the total amount of ATM crimes is rising, and believes that user awareness of the risk is the first line defence and delivering education and guidance to the citizens will reduce the risks [2]. Moreover, wireless networking technology is quickly changing the way networked computers work. The convenience offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired world. The security measures we have relied on in the past to secure our networks are now obsolete with this new technology [60]. It is therefore in this curriculum that we will introduce the encryption standards and the security issues surrounding it, whenever you are using a wireless network or you need to configure it at home or in the office. Additionally, despite the fact that everyone is aware of viruses and malware at least on a basic level, still a number of people do not realize the threat that phishing poses. Alternatively to phishing, every day email boxes being flooded with absolutely useless letters, therefore the spam has become extremely dangerous for computers and the users, especially for organizations. And online scamming is probably going to be the greatest threat in the near future, regarding this matter organizations and the users should be aware of all risks and threats, in fact that they are the targets.

Although workstations, laptops or home computers implement the latest updates such as operation system, antivirus, applications and so forth, still they are exposed to threats, regardless of what kind of applications or operation system is installed. Yet the computer cannot control what humans want to click on: to open or install applications, since people have a sense of control, they underestimate risks on the

Internet. Thus this section provides extremely effective and important information to everyday users of technology. Likewise it will deliver intriguingly best practice solutions of how to protect their computers, workstation, data, privacy, how to use the printing devices in a secure manner, followed by securing their portable and removable devices such as sticks, SSD, etc., including securing smart phones, how to use and create strong and safe passwords, how to use online banking, how to setup a secure wireless network and finally, how to identify online scams and spam. All in all, the section and the content will be extremely favourable and valuable for any type and size of organization, as well as for home users regardless of their usage and needs of technology and Internet. As a result, only significant changes in user perception, culture and education can effectively reduce the number of information and cyber security breaches.

In addition the following Chapter 3 objectives are to successfully deliver solutions for best practice of using technology, followed by how to protect personal as well as an organizations information, moreover to be aware and knowledgeable of how to configure wireless networks for personal benefits and eventually how to understand that you are the victim of an online scam and to interpret spam filtering. The curriculum is divided into three types of security approaches, such as: physical security, computer and mobile security; and network and Internet security. Firstly, the physical security approach shows very effective methods of protecting your personal and workstation computer, mobile and portable device protection, followed by extremely valuable secure printing issues. In addition, the computer and mobile device security approach deals with the malicious software, operating system security and how to create strong and safe passwords. At least, networking and Internet security module is carrying out the effective manipulation and deceiving people issue, such as social engineering and social networking; important to every day secure browsing, with solutions on how to identify phishing and perform successful online banking; identifying annoying spam e-mail and instant messaging messages, followed by firewall and wireless network security, on regular performance.

Nevertheless, Chapter 3 discusses the possibilities of securing the different purpose needs and also delivers best practice solutions to reduce the number of threats in the use of technology, be it the workstation, laptop, home computer or mobile and portable devices. We address and stress human habits that they are unaware of that cause and risk, the very valuable assets of the stakeholder.

2.2 Advance

The end users of computers are rapidly growing in leaps and bounds. Their control of computers is increasing too. Tutorials, studying, experimenting and learning environments are available for free and they lead to end users of technology to figure out comprehensive software, and to take full control or functionality of software, network, testing, analysing, developing and so forth. Although the enhancement of technology and Internet suits the daily demands, commitment and performance of advance users, there are many ways to circumvent the defence. In this matter, if the users are advanced or professional in computers, they are aware that they can be targeted as victims or exposed to risks. It is therefore extremely important and favourable that an awareness activity is taken into account. By determining that advance users or in other words experts of computers are in fact the ones that can perform and carry out activities such as, configuring networking, programming, troubleshooting issues, installing, etc.

However, this curriculum presents an overall anatomy of an attack and a taxonomy of the tools appropriated in this process; it provides literal scenarios of hacking activities and the solution of defence against the attacks. Taken as a whole, it provides a reasonable tactical model for the process of sketching and constructing an attack, complemented by a technical overview of the tools, exploiting the steps employed in this process and finally a resolution. The general framework of attacks against computer systems standards are usually described, in approaches such as [67] and [51] where they aid in delivering the framework, where on the other hand we prefer the curriculum to divide the targeted phase attacks into the following components:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining and Expanding Access
- Covering Tracks and Hiding

In addition, we supply the participants with additional very attractive and valuable types of attacks, where each type of attack is followed by countermeasures:

- Network Scanning Attacks
- Password Attacks
- Exploitation
- Web Application Attacks

Alternatively, for the attacking phases and attacking methods, we supply the participants with APTs, like anatomy and how to improve resilience to APTs in organizations.

Furthermore, we emphasize on the risk assessment element as a step in risk management procedure to identify, prioritize, and estimate risk to an organization's operations, assets, individuals, and other interconnected organizations.

We have to keep in mind that a security incident happens when we have a threat (i.e. attack) and at the same time vulnerability (i.e. no protective / meditative measures implemented against this concrete attack).

$$R = P_{robability}\left(T \cap V\right) \times L$$

Where the:

R is risk that could be function of threats intersect of vulnerabilities,

P is defining the probability of: T defines the threats intersect with V - vulnerabilities and

L is the loss caused by a security incident.

However, to be more precise in details the purpose of the risk assessment element is to identify and evaluate the following:

- Threats for operations, assets, or individuals
- Vulnerabilities same as above
- Impact for the consequence, losses or opportunity and
- Probability or, even better, Frequency of security incident occurrence

The reason why it is better to use Frequency is that, for example, in calculating the risks for a year, if the security incident takes place once a year then Probability=1 and if the security incident takes place once a month then still Probability=1, but in reality the sum of losses will be very different, i.e.:

$$R = F_{requency}\left(T \cap V\right) \times L$$

Thus, the advanced curriculum, will guide the end advance users of technology to identify the leaks into their system, and hence take action for countermeasures, in information security. Nowadays, the productive applications are more often pursued on the web where access can be gained globally. It is therefore, important to understand the attacking phases, followed by the type of attacks and eventual protective measures and also the anatomy and the countermeasures of APTs. Securing information security assets is an essential and extremely important value for stakeholders.

Ultimately, in Chapter 4 we deliver the curriculum of the advance course, where the above attacking phases and attacking types are discussed and the countermeasures to secure your assets for each type of attack, and the APTs anatomy and countermeasures are provided. Eventually, we examine what risk and incidents to avoid, if it is not possible to avoid the incident, we then provide the possibilities of how to mitigate the security incident.

2.3 Management

Managers and staff are constantly faced with increasing levels of complexity in managing the security of their organizations and in preventing attacks that are increasingly sophisticated. In fact as individuals they are subjected to enormous amounts of information across broad ranges of subjects, such as, security policies, new technologies, new patches, new threats, and new sources of information, and the list is endless. To be able to fulfil the function of their role in the organization whether at a strategic or tactical level they make many decisions each day [27]. As the environment continues to become more dynamic and complex the process of making good security decisions is becoming extremely challenging. Therefore, creating or delivering a security awareness culture in organizations depends on improving how managers or individuals make security decisions. The awareness Management curriculum of our decision-making processes can help improve decisions and promote a security awareness culture in organizations.

Obviously, all managers are users, where on the other hand all users are not managers. Thereby, the novel approach of the course curriculum is to deliver to the participants decision making process phases. The aim is to deliver knowledge of managerial decision making in organizations, which is regarded as the core of an organization's operation and the foundation for any top-level executive. Throughout this course, we will introduce four perspectives phases in the study of individual, group, and organizational decision making and approaches under these perspectives. We will consider the role of rationality and non-rationality in managerial decision making and examine how uncertainty and ambiguity may impact managerial perceptions of choices and risks.

Furthermore, cost optimization and limitation of resources is a key goal in management today, and yet they still need to avoid costly information security breaches. With this in mind our management curriculum will focus only on approaches of decision making process in the first step and eventually in optimization. A decision making process is a method by which an entity makes decisions. It can be a formally specified routine or an unspecified ad-hoc approach. Regardless of formality and strategy the decision-making process is often conceived as a two type of four-part cycle of observing, orienting, deciding and acting - the *OODA loop* [38][10] and four-part cycle of plan, do, check and act - the Deming circle [7] or *PDCA* [13]. Although there are two specific OODA loops: *BMD OODA loop* and *Cyber OODA Loop* [38] we discuss in this paper only the relation to cyber attack defence domain.

Therefore, in Chapter 5 we examine important facets of the decision-making and provide prescriptive guidance on how the quality of decision-making processes may be improved thus leading to better security decisions within two phases of the decision making process.

2.4 Further Improvement

On one hand the syllabus at the moment consists of best known practice and answers to the questions, what to do to be secure and aware. On the other hand, it could involve how to avoid risks, and what risks are possible to mitigate. Delivering an awareness program to a wide and varied audience is not an easy task. At this time, the syllabus essential character is separated into three groups: basic, advance and management. Future extension of the syllabus courses could engage the participants and different IT users and groups with knowledge as follows:

- Development. Although in advance course curriculum we noted the programming techniques and how to proceed within countermeasures of coding mistakes, we still consider that by separating and adding more details, the development curriculum will lead the development of applications to be developed in a better manner, and in a deeper defence line. The initial idea is not to teach and deliver to the participant how to program from the start, but in fact it will consist of how to make safe applications, in several common and well known programming languages. For instance, the content of this course could include courses like those taught at Tallinn Technical University such as principles of secure software design, secure programming techniques, applied cryptography and many others. Those examples will help and assist the developers of application for organizational needs to meet the security requirements and to raise the level of defence. In more detail, the cryptographic algorithms will contribute to fulfil the need to encrypt the data or protocol. Additionally, understanding the principles and secure programming techniques will serve for better procedure and better techniques of development in the current application, for both web application and desktop application. In addition, another importance is to add the licensing terms and types, what type of license should be chosen for the application and shared, either with an open source license or with a commerce license.

- Youth and parents course. Many organizations and states nowadays are expressing the importance of the young generations to use everyday technologies. Many real life scenarios have occurred where a predator through social networking sites victimizes youth. Because of this critical issue, we could develop a separate course curriculum, where to inform and teach parents and younger generations how to act and to identify the predators. How to configure parental control and so forth. For instance this can be done by developing a future content of social networking techniques and Internet psychology.

- Legal and Policy Aspects. By focusing on the legal and policy aspects of the cyber security: both the organizational, area, state and international aspects. Criminal law, information security, electronic communications. International cooperation. Soft-law. Conceptions and terminology.

3 Basic

We examine and emphasize the importance of three types of security issues that can occur as security breaches, whether the participants are using technology in the office or at home. For instance, physical security, computer and mobile security and network and Internet security. In addition we deliver possibilities for further improvements to the basic course curriculum. However, we consider that for an everyday user of technology, it is enough to have a course about IT security which will deliver what to do as the best practice and how to countermeasure and bypass the attack.

Moreover, each type of security measure illustrates the best practice and the kind of approach should be taken into account to protect your data, mobile or portable and removable devices. Additionally, it tackles antimalware, or antivirus solution issues, what it provides protection from and how to perform and operate within your operating system; how to create strong passwords and where to keep them safely. Alternatively, the course provides an example of threats that can occur by using every day social networking, by social engineering and how to identify phishing and spam; how to protect your home or workstation network and configure secure wireless networking.

In the current chapter we outline the terminology of three types of security issues, followed with subsections for securing different vulnerabilities and assets. Finally we conclude with the further improvements to the curriculum.

3.1 Physical Security

Physical security is the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, institution or personal assets. This includes protection from burglary, theft, vandalism, etc. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker [59].

Therefore, we provide the participant in this module with the best practice on how to protect their computer by locking it, how to setup a password screen saver and how to act in regard to social engineering. Moreover, we inform them on how to protect their data by backup, data encryption and secure their removable devices. In addition we provide them with security countermeasures and best practice of security for their mobile and portable devices, followed by how to change their behaviour or bad human operation habits of leaving printed, scanned or faxed information that can be mistakenly viewed.

3.1.1 Protect Your Computer

Today computers are operating within a complex networked environment. As end users within such a network, we will have to ultimately face our actions and habits while using and working in the office and home computers on a daily basis. The intent of this unit is to assist and illustrate to all users what should and should not be done, along with best practice scenarios. Additionally we will illustrate what can happen if the computer allows access to anyone.

However, when we work with our computers, especially in networked computing environments, we tend to carry a bunch of human operation habits. For instance, leaving the computer logged-in, leaving programs running, or even leaving our email client open and the software running, can cause a lot of grief to not only the computer system we use, but also the network it connects to and communicates with [48]. Thereby, the most important layer in securing the computer and the workstation is by protecting the computer by locking it, configuring a password screen saver and knowing how to respond against social engineering. Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking methods [25]. If the computer allows anyone to turn it on and use it, any or all of the following can occur: identity theft, loss of important information and/or entire files and fraud. These are a few of the reasons why it is important to configure computer to ask for a password before it can be accessed and by locking it when stepping out of the home or office.

Moreover, when the office computer and laptop are left constantly logged in, especially during times when a person is away from the office or table, the computer and its electronic contents are exposed to unnecessary personal security risks. Consequently the thief will have access to personal data, payroll data, company documents and the network. Therefore, it is vital to consider a unique username and password as being no different than your Bank ATM card and PIN code [48]. Alternatively, when leaving programs (or multiple programs) running on a computer allows the thief to see applications and tasks that are running and this can facilitate the process of gathering information. Leaving the e-mail program open and running, also poses an unnecessary personal security risk, where the thief can send any mail from this computer and it will be interpreted as coming from you. Hence, it takes only a few seconds for the thief to eviscerate data, information, etc. from a computer. The same as it takes only a few seconds to secure your computer. Thereby we illustrate two recommendation methods to successfully secure a computer:

1. Lock down the computer manually

2. Set a password protected screen-saver

Despite the password security and computer locking techniques, still human behaviour obviously can lead to mistakes, and the involuntary sharing and leaking of personal or an organization's information. For instance an attacker could impersonate legitimate users and request a password, or information of existing technologies, or account reset, or access to the building, or request information details over the phone and so forth. Consequently the exploitation of the weakest vector of human element nearly always works. Therefore, the organization should implement awareness guide and program on how to reduce the risk of social engineering attacks, however in this paper we suggest only the most known best practice on how to bypass social engineering vulnerability and exploitation in the physical aspects. How to countermeasure different types of attacking approach linked to protecting the computer. The information nevertheless should not be shared under any circumstances, for instance, by phone with the IT department requesting passwords or credentials, the employee should make sure or ask the supervisor to gather more information on if to share or not.

The final recommendation is to never share or leave or distribute your own password or username and, always the lock the computer when leaving your desk. Alternatively setting up a password screen saver, helps to protect information and applications that are running on computer. Moreover, always be aware and double check the person that has asked for personal information, such as username or password with the managerial team or ask for the reason why this information or task is requested.

3.1.2 Data Protection

The growth of using technologies everyday has drastically made it easier to collect and maintain information about individuals and organizations. An accompanying growth in incidents of loss and unauthorized use of such information has led to increased concerns about protecting this information, whereas the escalation of security breaches involving personal identifiable information (PII) has contributed to the loss of millions of records over the past few years [23]. Indeed breaches involving PII are hazardous to both individuals and organizations. Therefore, we help individuals and organizations to take appropriate protection measures of their confidentiality by informing them on risk-based approaches. The goal of data protection is to protect the rights (particularly rights to privacy) and fundamental freedom of individuals with regard to automatic processing of their personal data. However, in this section we will provide best practice solutions of backing up informational data, followed by how to protect your systems by implementing encryption of data and additionally how to protect your removable devices. Moreover, backup or the process of backing up is making copies of data which may be used to restore the original after a data loss event [15]. Likewise, data loss or stolen data can entail a great loss or sacrifice not only for organization but for individuals too. Nevertheless, all computer data is at risk from threat or damage, even with the use of the most reliable equipment and in the most secure operating environment, there is always the possibility of something going wrong. Additionally, another step of protecting data should implement data encryption, which is an algorithm for the encryption of electronic data, which provides access to data after requesting passwords and provides different algorithms. Also extremely important is to protect removable media, in other words, storage media which are designed to be removed from the computer without turning the computer off, or devices that we carry everywhere, such as USB flash drives, external hard disks, optical discs, memory cards, iPods, Bluetooth, etc.

We annotate the extreme importance and intriguing best practice solutions of awareness and protection of personal and organizational data. Finally we illustrate how to encrypt sensitive and on the other hand valuable data by highlighting the importance of protecting the most exposed and vulnerable data, such as the removable devices.

3.1.3 Mobile and Portable Device

The rapid diffusion of mobile telephony, Internet and broadband networks all demonstrate how pervasive mobile and portable technology has become. The penetration of mobile phones and portable devices has been particularly intensive and in recent years they have become an essential technical device, for personal usage and enterprise organizations. Additionally, as users store more and process more and more data including sensitive information in their phones (e.g. private photos shot by the phone's internal camera, an organization's documents or personal credit card numbers and PINs) their security concerns grow [6]. Moreover, recent Checkpoint [46] analysis highlights that 71% of companies today literally consider mobile devices, as a matter of fact the most incisive cause of security issues into their organization.

Regarding this matter, in this section we point out the importance of utter protection of mobile and portable devices known as small hand-held computer devices; devices that have a processor, or in other words devices that typically have a display screen with touch input and/or miniature keyboard, for instance, PDA, smart phones/mobile devices, laptop/notebook, etc. They are devices that are usually always carried on the move and they connect and communicate in different networks through modes of connecting to the Internet. However, along the way, they collect all kinds of information, from personal contacts, messages, financial accounts, and so forth. Therefore, if we are aware of how to secure computers or credit cards, we should be aware and take into account how to protect the mobile and portable devices too.

Because of this we show the best practice of physical security measures on how to secure and give solutions on what to protect in the mobile, tablet, notebook and laptop devices.

Nevertheless, we emphasize the persuasion of securing the portable devices primarily to establish an acceptable use of policy, as password protection of mobile and portable devices that is the first line of defence. Next, to encrypt data, we provide several tools such as, for Android like Whispersystem[1], for iOS[2] and so forth. In addition, the malicious code and viruses are growing constantly for mobile and portable devices, therefore, major antivirus vendors now support mobile platforms and provide a variety of tools and applications such as antivirus, anti theft and anti spyware solutions. Alternatively to virus and password protection, a best practice when connecting through Internet or corporation network we recommend could be to use a firewall and VPN solutions for different platforms.

3.1.4 Secure Printing

Security printing deals with the printing of items, business and transaction documents and the main goal of security printing is to prevent forgery, tampering, or counterfeiting. Therefore, this factor underlines the fact that document printing and copying are often mistakenly viewed. New printing technologies and applications in fact provide ways for companies to improve customer communications, cut spending and streamline business processes but at the same time expose organizations to security risks and threats [21]. It is therefore crucial to employ good practice to comply with existing regulations and secure printed information [8]. Emphasizing document security on printers and multifunction products is an issue within corporations [17].

This unit gives a brief outline of the data which is susceptible to security breaches and incidents, where we highlight potential risks associated with document copying and printing, and provide the participants with a good practice guideline which aims at helping them to overcome secure printing obstacles within their organizations. We do not cover the legal aspects associated with this topic. Therefore, for this purpose and matters we have applied the recent Security Printing ENISA book [40].

Printers and copiers produce the bulk of hard-copy personal information and business output, such as invoices, forms, transactions, tickets, statements, employee documents and customer data. Thus, often sensitive data is most vulnerable when in transit between the user's workstation, laptop and the printing device's output tray, especially when printing remotely. It is therefore necessary to emphasize that printing devices are a powerful link within the overall security chain, subsequently where multiple function printers provide features such as scan-to, emailing and faxing. All in all, these devices and the documents remain largely unprotected, where leaving business, personal information and transaction documents printed can yield to security breaches. This is why security on printing and copying products is an issue with enterprises and even home users [65].

[1] Whispersystem: http://www.whispersys.com/, last checked 17.04.2012

[2] iOS: http://support.apple.com/kb/HT4175, last checked 17.04.2012

Secure printing is any step taken to ensure that:

- printing device will remain secure;
- printed or transmitted data will remain:
  - Confidential - Ensuring the information is accessible only to those authorized
  - Integral - Protecting the accuracy and completeness of information
  - Available - Ensuring the access to information is available when and where is required and is not denied to any authorized user.

Furthermore, security standards will help and guide in complying with the three above-mentioned aspects of security and some security standards comply with best practices and controls related to secure printing matters, such as following: ISO/IEC 27002:2005 [29], PCI data security standard (DSS) Version 2 [44] and COBIT [1].

However, the following organization assets were identified in terms of secure printing:

- physical assets: printing, fax, email devices;
- people: employees, contractors, visitors;
- software: intellectual property rights (IPR) and patents;
- data printed, copied and transmitted.

All in all, we annotated the importance and extreme value of the assets. Printing can be used to target organizations. However, we only mention the standards for a future action and we do not go through the details. And finally we illustrate the best practice solutions to the participants of securing the printing issues.

3.2 Computer and Mobile Security

Computer and mobile security is a section where we explain how to setup and perform usage of computer or mobile device to reduce the vulnerability and how to follow the latest updates, and patches implemented into the system. Furthermore, updates mean to bring the current software or system up to date, such as updated version of the operation system or the latest application. In addition, patching is a software only designed to fix problems [14] with, or update a computer application or its supporting data. For instance, it includes fixing security vulnerabilities and other bugs, and it improves usability or performance. However, by installing third party software in a computer or mobile device it conveys additional vulnerabilities. As a result, by constantly updating the operation system, applications, etc. will help in improving and protecting electronically devices, moreover by installing an anti malicious software the security level is increased. Another security issue is to be able to create a strong and difficult guessing password and secure the system password.

In this section we will illustrate to the participants to be aware of best known practice, how to protect their computers and mobile devices by making them less vulnerable by installing third party software such as anti virus and anti spyware, additionally what is the best known practice to exceed the security of operation systems either on their computer or portable devices for instance tablet or mobile/smart phone devices. Closing by, providing the best apprehended solution of creating strong passwords and how to keep the password save.

3.2.1 Malicious Software

Over the last four decades, since the first recorded virus Creeper in 1971 [33], malicious software has evolved from occasional "exploits" to a global millionaire criminal industry [42]. Malicious software or in other words malware is any software that gives partial to full control of your computer to do whatever the malware creator wants. In fact the main purpose is to harm the system or other systems, or to subvert them to uses other than those intended by their owners. Malware can be a virus, worm, trojan, adware, spyware, rootkit, etc. The damage done can vary from something slight as changing or deleting documents to full control of the system without the ability to easily find out this control. Most malware requires the user to initiate its operation. However, some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after clicking OK on pop-up windows, and from vulnerabilities in the operating system or applications [19]. In addition, spyware is a malicious code that collects information about the users without their knowledge, for instance they can perform as a key logger and may be installed by the owner of a shared, or public computer on purpose in order to intentionally monitor users, which exposes information about the network and activities. Furthermore, malware is not limited to one operating system and it affects all actors. Different from computer malicious code, mobile malicious code could pose a greater risk for losses than computer malicious code, say scientists from Rutgers University [22]. For instance they can send messages, dial phone numbers, forward mobile banking information, carry out data theft, and moreover, spyware can record or send audio, video, pictures, can share one's location and so forth. It is increasingly a shared concern for businesses, governments and individuals.

Moreover, malware types can be categorized as follows: viruses, worms, trojans, and backdoors that seek to infect and spread themselves to create more havoc; adware and spyware that seek to embed themselves to watch what the user does and act upon that data;. Rootkits that seek to give full access of your machine to the attacker to do what they want [19].

It is therefore, extremely important and valuable for organizations and individuals to be aware of what to secure and how to secure it. Furthermore, in case of infection, installing third party software such as antivirus and antispyware will assist the organizations and individuals to protect both computers and mobile devices against malicious software. Therefore, in this section we provide the participants with best known practice of antispyware and antivirus solutions. Besides antispyware and antivirus we provide additional protection tools that can limit Internet connection to deny unauthorized access in the Network and Internet Security section.

3.2.2 Operating System Security

In the earliest electronic digital computers, operating systems(OS) were unheard of and programming languages were unknown, but in the 1940s the first generation of operation systems was issued [39]. Therefore, operation systems and programming languages are an essential part of computer and electronic devices. Nowadays operating systems are a vital component and provide a set of functionalities needed and are used by most application programs on the computer and the linkages to synchronize computer hardware. In other words, the operating system is a set of programs that manage the computer hardware resources and provide common services for application software. Also today the operating system is an essential component of mobile devices too, for instance controlling and performing calls or sending messages by touching the screen or button on the mobile phones. Examples of operating systems are: Unix[3], BSD[4], Mac OS X[5], Linux[6] or GNU/Linux, Microsoft Windows, etc. and for mobile devices Android[7], Microsoft Windows Mobile[8], iOS[9], Symbian[10], etc.

Operating systems are made up of countless parts with different functions and operations ideally working in harmony. Yet it is inevitable that some of those parts are less than perfect. But when a problem occurs and leaves a hole in the system's defences, it is extremely important to patch it as soon as possible. Remarkably as systems are used and new technologies are released, OS requires software patches and upgrades to resolve any security issues that are discovered and to improve functionality and performance. Despite that most of the operating systems nowadays are configured by default to perform automatic updates, yet human bad habit disables this function, and in the end the system and the applications are becoming in fact vulnerable to exploitation.

As a part of any electronic device, it is essential fact that novel action should be taken into consideration of protecting the operating system. For this reason, we

[3] Unix: `http://www.unix.org/`, last checked 17.04.2012

[4] BSD: `http://en.wikipedia.org/wiki/Berkeley_Software_Distribution`, last checked 17.04.2012

[5] Mac OS X: `http://www.apple.com/macosx/`, last checked 17.04.2012

[6] Linux: `http://en.wikipedia.org/wiki/Linux`, last checked 17.04.2012

[7] Android: `http://www.android.com/`, last checked 17.04.2012

[8] MS Windows Mobile: `http://www.microsoft.com/windowsphone/en-us/default.aspx`, last checked 17.04.2012

[9] iOS: `http://www.apple.com/ios/`, last checked 17.04.2012

[10] Symbian: `http://symbian.nokia.com`, last checked 17.04.2012

provide the participant with a solution and purpose action plan, such as, to use security software, to maintain current software and updates and patches constantly for both devices computer and mobile as to be able to carry on with significant productiveness of everyday work, valuable for organizations or individual.

3.2.3 Strong and Safe Password

Access control to computer and mobile devices is often implemented via password; hence, attacking the password is one of the most straightforward attack vectors. Typical computer and mobile users nowadays require passwords for purposes: logging into the system accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, e-banking, etc. Furthermore, a password is a secret word or string of characters that is used for authentication in order to prove identity or gain access to a resource. The password should be kept secret from those who do not have allowed access [56]. Password or watchwords have been used since ancient times in the Roman military system [24].

Most people know that the first line of defence is a strong password, yet they still do not change the password frequently or create a strong password that is difficult to guess. In addition, they are not aware of the methods and the possibilities of creating a strong password. The consequences are that if the password is weak the thief will gain access to the entire network, or application or documents of organization or individual, especially in mobile device where it can make calls or send text message or exploit privileges. Alternatively, often one of the bad human habits is to leave the password on the desk written on the paper or in a drawer, which is accessible by anyone. In addition for mobile devices they are many different ways of protecting your device, either by password, SIM card PIN code or for instance Android OS provides the users with possibilities of using the visible pattern or tactile feedback for security.

Besides distributing the countermeasures, additionally we show noting password guessing methods, in other word how passwords can be stolen. By knowing the tactics of how passwords are stolen, will assist for the participant to produce a strong password strength. The most known and frequently used techniques that we deliver to the participants are the following:

- Guessing - by collecting and gathering personal information found from different sources, for instance online: names, birth dates, pet names, etc.
- Dictionary - based attacks - word lists or dictionary, that can be run against user accounts, and if the password is a simple word, it can be found pretty quickly.
- “Brute Force” attacks - it is known as the most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

- Rainbow tables - use refined algorithms through a number of different reduction functions create multiple parallel chains within a single rainbow table, reducing the probability of false positives from accidental chain collisions, and thus increase the probability of a correct password crack.

For this reason we suggest the guidelines for creating and using strong passwords, and we point out the importance to be given to shoulder surfing. For instance, when typing the password into the computer someone can be watching the username and password entered and which can be exploited later. Finally, the strong password and its safe storage is undeniably an important value of any organization and individual to protect your system, device, application, etc. from being accessed by anyone.

3.3 Network and Internet Security

The history of computer network began with the development of computers in the 1950's. The first step was the point-to-point communication between mainframe computers and terminals. The development further expanded in 1982 and it was standardized by Internet Protocol Suite (TCP/IP) and the concept of a world-wide network of fully interconnected TCP/IP networks called the Internet. The 1990's brought with it the dawn of the modern information security industry, where notable threats were witnessed during this decade [35].

Furthermore, network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs, conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and or can be open to public access. Network security involves organizations, enterprises, and other types of institutions. Its title is explicit: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [5].

In this section, firstly we introduce the participants to social engineering and social networking issues that can arise from the use of the network, whether it is private or public, and the use of Internet social networking sites. Secondly, we illustrate best known practice of secure browsing, followed within secure online banking and in addition how to identify phishing. Then we deal with how to identify spam and secure best practice through instant messaging. We also explain best known practice of securing and configuring their network by setting the firewall. Finally we show how to use, setup and perform secure wireless networking.

3.3.1 Social Engineering and Social Networking

Although there are many ways online criminals can use sophisticated technology and try to gain access to computer, one of the simplest and more insidious is by social engineering. Social engineering is a way for criminals to gain access to computer. The purpose of social engineering is usually to secretly gain access to computer and install spyware or other malicious software or to trick people into handing over their passwords or other sensitive financial, organizational or personal information.

Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Frequently, social engineers will search wheelie bin for valuable information, memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed [58].

On this subject security experts propose that as the culture becomes more dependent on information, social engineering will remain the greatest threat to any security system [58]. As a result we provide education assistance on how to protect valuable information and to increase the participants' awareness of how social engineers operate by providing the best known practice and methods of online threats that social engineers use.

Furthermore, social networking sites like Facebook, Twitter, LinkedIn, Youtube and so forth have become popular playgrounds for attackers who recognize user's tendency to instil a higher level of trust in the sites themselves and to share too much personal information. In fact, according to the Sophos Security Threat Report 2012 [52], there was a 67% rise in proportion of organizations that report encountering spam and malware attacks via social networks, and using personal laptops or phones to access company resources remarkably increases the risk of data loss to 74%.

It is therefore extremely important and valuable to educate and increase awareness in everyday work with social networking. In this unit we provide and illustrate the best known practice and solution of bypassing the attacks via social engineering as well as via social networking sites.

3.3.2 Secure Browsing

The first browser was invented in the early 1990s, it was called Worldwide Web [9]. And today the initial idea has expanded and changed. However, a web browser is a software application for retrieving, presenting and traversing information resources on the Web.

In this section we help participants to gather information on how to configure a web browser for a safer Internet surfing. The guide serves individual and even organizational purposes. Additionally we illustrate the way of identifying the phishing scams. Therefore, we deliver how to identify the main ways in which a phishing attack can affect, describe ways to tell a phishing attack from a legitimate website, moreover, to identify ways to avoid becoming a victim of phishing attacks, and in the end explanations on what to do as the victim of a phishing attack. Furthermore, we note how to be secure while performing online banking.

Moreover, attackers focus on exploiting client-side systems through various vulnerabilities. Thus vulnerabilities to take control of computer, steal information, destroy files, and use it as a vector to attack other computers on the network.

However, all the above can be avoided by using the secure browsing layer - HTTPS, and it is a combination of HTTP with SSL/TCP protocol. Moreover, SSL is a cryptographic protocol that provides communication security over the Internet [16].

By providing and learning how the participant should secure himself, it raises the awareness and excluding security vulnerabilities of using browsers every day, either on a personal computer or a workstation from an organization.

3.3.3 E-mail and Instant Messaging Security

Amplification of the late 19th Century of sending telegraphic messages to a multiple destination, today is advanced in using electronic systems to send unsolicited bulk messages [18]. Meanwhile, the most widely recognized spam is e-mail spam, the term is applied to similar abuses, such as: instant messaging spam, newsgroup spam, web search engine spam, spam in blogs, spam in wiki, mobile phone messaging spam, social networking spam, etc. At this point, many of e-mail boxes are flooded with absolutely useless letters, which in fact are extremely annoying. Furthermore, most of the spam either contains malicious codes, or redirecting links which will ask for personal information such as, entering username and password, or by opening the spam e-mail will automatically execute software which will send e-mails to the entire address book contacts. As a result all the contacts in the address book are infected. Therefore, organizations and individuals should take action in preventing and identifying spam, by knowing how to apply filters and the procedure of reporting spam. This would increase the level of reliability and vulnerabilities in organizations and even for individuals. Due to this fact, in this section we illustrate to the participants how to identify spam in e-mail and additionally instant messaging.

Then we provide with the best practice on how to apply filters and eliminate unwanted bulk mail. And finally, we note the procedure of reporting spam. Hence, we conceive that in this area the individuals and organizations will be more secured.

3.3.4 Firewall

One of the most important ways of staying safe online is by protecting both incoming and outgoing network traffic. Network traffic is easy to exploit, for instance to install malicious code, destroy files, cause malfunctions or even cause an online virus to proliferate to understand the technology of the entire organization, and so forth.

A firewall is a security system, consisting of a combination of hardware and software that limits the exposure of a computer or computer network from attacks by crackers; commonly used on local area networks that are connected to the Internet; some of the firewalls can help and the same time prevent hackers from using the embattled computer to lunch attacks on other computers. Additionally, firewall is designed to monitor the transfer of information to and from the network. While firewall protection is essential, it is also important for the participants to understand what a firewall can and cannot do.

Therefore, we showed to the participants how to determine the best overall approach to network security, consider what firewalls can and cannot do to protect their workstations or personal computers and additionally illustrate the firewall basics.

3.3.5 Wireless Network Security

Wireless network refers to any type of computer network that is not connected by wire of any kind and it is not an alternative to wired networks. The idea behind the wireless network was to reduce the cost of installation of cables in a building. However, there are many types of wireless networks, in this section we will only concentrate on Wireless LAN network (WLAN), in other words wireless local area network. WLAN links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access [53], within different specifications and standards.

Moreover, wireless vulnerabilities can be illustrated, such as: password guessing, wireless network encryption (WEP and WPA), media access control (MAC) address spoofing, etc. All the vulnerabilities can be applied into an organizational environment network and even to the home network. It is therefore, extremely important and valuable to demonstrate the implementation of securing the wireless network.

As a result, we illustrate to the participants the best practice scenarios of how to secure wireless network, for example: encrypting communication over the network, changing the router's identifier from the default and changing the default password and how to identify if the public hot-spot is safe to connect to. And additionally, we provide a brief overview of specifications and standards of WLAN.

3.4 Further Improvement

The concept of security awareness program of the basic course curriculum could be extended and developed in more specific directions to accompany general security awareness efforts for curtain organizations or even for governmental organizations.

Indeed, such training is mandatory on a recurring basis. As a result, we could consider the following ideas of improving the future development of the basic course:

- Social media and social informatics and additionally Internet psychology. Understand the growing power and utility of social media and networking in everyday lives, the benefits and risks of social media and networking and how to use them safely at work and at home. Additionally, by delivering the basic understanding of Internet psychology, what could happen and what did happen with real live scenarios.
- Information security responsibilities, principles, and policies. Provides an understanding of what information security is, why it is important, and identifying the person responsible for information security.
- Legal Aspect. What legal aspects should be considered and taken into account before taking any action and what the consequences will be. Undertaking into consideration the legal approach of state or nation law enforcement and implementation.

4 Advance

In this curriculum we deal with presenting to the advance, expert users of computers how to be conversant with more in-depth details of threats and defence in security. Primarily, we emphasize the five attacking phases. The aim is for participants to understand the attacking phases, such as: reconnaissance, scanning, gaining, maintaining and expanding access and finally covering tracks. Apart from illustrating the attacking phases we demonstrate various scenarios of attacks that could occur. In more detail, firstly we introduce the participants with the network scanning attacks, with port scanning, host discovery, operating system version detection, vulnerability scanning and finally we give scanning countermeasures. We next move on to password attacks, followed by type of password attacks and concluding with countermeasures. Thirdly, we explain the exploitation types followed by how to protect against exploitation. And finally, with the most common known attack today on web applications, for example code injection, SQL injection, session management and path traversal attacks; cross site scripting and cross site request forgery attacks and in the end we talk about web application countermeasures. In addition, we note the anatomy and countermeasures of advanced persistent threats and provide a list of recent to older significant attacks.

In the current chapter we outline the attacking phases, followed by the various types of attacks and the subsection we expose the numerous techniques and recommendations of what countermeasures should be taken into consideration for certain types of attack. Meanwhile, we illustrate the anatomy of APTs and how to improve resilience to them. The last step is the further improvement of the curriculum.

4.1 Attack Phases

Although Ed Skoudis and Tom Liston [51], and Susan Young and Dave Aitel [67] n their books introduce the anatomy and taxonomy of attacking phases frameworks we prefer to use different target phases of activities, so as to be able to simplify and adapt them to a more understandable form for a wide range of users, and to deliver best awareness knowledge of extremely important elements of the attacking phases.

Therefore in Figure 4.1, first, we introduce the reconnaissance, by delivering the attacking types of social engineering and direct interaction with the system. Secondly, we expose the scanning phases, by providing the different attacking types, such as network scanning, vulnerability scanning and explain web application mapping.

Thirdly we explain how the attacker is gains access of the system, for example as Denial of Service; and session and path hijacking. We then introduce the participants with the fourth stage, on how the attacker maintains, expands access and exploits the system and then covers their tracks by using two solutions such as tunnelling and proxy over the network.

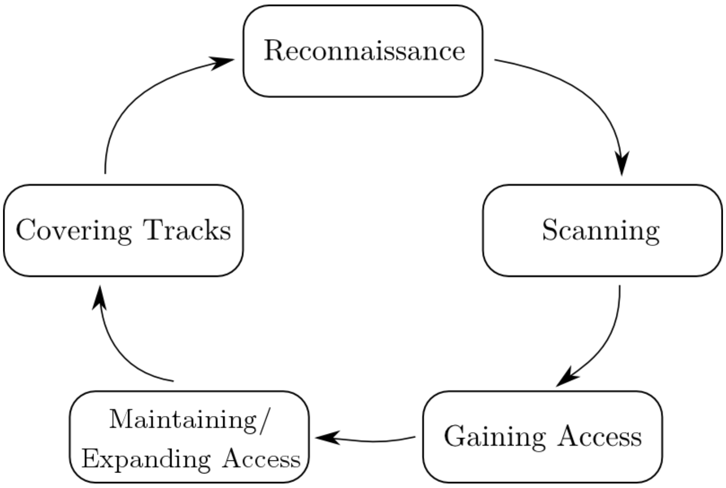


Figure 4.1: Attacking Phases

In the following sections we describe each of these activities only by the possible tactics, rather than by illustrating their defence solutions.

4.1.1 Reconnaissance

To improve the efficiency of the attack and its probability of success a hacker has to know and get as much information as possible about the target system and the details of its strong and weak points. The information is important for the hackers, and they rarely attack an organization's network before profiling and collecting enough information about the targeted network, system and administrative staff.

Some types of reconnaissance can be detected by a target organization, for instance social engineering or site reconnaissance activities, where the majority of resources are gathered by Internet search engines and complete anonymity and legality of the perpetrator.

Overall, the goal of the hacker during the reconnaissance is to improve the probability of gathering details and the odds of successfully masking their identity. However, enumerated information could be obtained by using different techniques and activities. We categorize them into two activities below:

- Social engineering in other words no direct interaction with the system. It refers to a reconnaissance activity of gathering useful data by requesting the information from an employee or contractor of the targeted organization. Moreover, a mass of reconnaissance information can be gathered from the Internet, directories, yellow pages, etc. Generally, social engineering reconnaissance is achieved by manipulating an individual to persuade them to release information to an impostor, alternatively by using the search engines to collect information such as, employee names from social networking services like Facebook and LinkedIn; business partners and existing technologies. Consequently, the perpetrator will be able to create, contrast and assemble the puzzle of the organization for a future action. Mailing lists sometimes reveal information about existing problems and configurations of IT systems.

- Direct interaction with the system, such as IP and technical reconnaissance needed prior to in here in targeted systems and services for attack activity. For instance, gathering access to the targeted building and infrastructure, understanding of the host and network IP information. Where IP and DNS information can be obtained by doing simple WHOIS searches and forward and reverse DNS requests using tools like *dig*, host and *nslookup*. Identifying employees' e-mails, phone numbers, in addition gathering physical connectivity of networks by entering the building. Collecting details of operating systems and their applications that are currently running.

In this phase the attacker's idea is to gain extremely useful insight information of the target organization and infrastructure, which will help to build the blocks for the next phase of the attack, scanning.

4.1.2 Scanning

After the stealthy reconnaissance phase, when the attacker is equipped with some vital information about the target organization comes the time for more aggressive and intrusive target mapping. The purpose of this stage is to gather an information base about the target system, such as host and open ports, network scanning and network mapping. The attacker then identifies which of them are potentially vulnerable and defines the web applications running and mapping follows. The process consists of the activities explained below:

- Network Scanning. The idea behind network scanning and enumeration is to literally gain insight of the network, for instance, IP addresses of hosts that are accessible, to identify open TCP and UDP ports, as well as to identify what applications are running on those open ports, the versions of running services, known of operating system versions and to target system users and shared folders. Moreover, configuration of firewalls and other security systems such as IDS software [36, Ch. 4]. For this purpose the intruder can use several scanning tools and techniques.
- Vulnerability Scanning, is to identify known vulnerabilities in known network services and applications. By using a vulnerability scanner as an effective and fast way of determining the security holes and status of the targeted system

different tests can be executed. Tests can be safe or intrusive. An intrusive test tries to exercise the vulnerability, which can crash or alter the remote target. On the other hand non-intrusive tests try not to cause any harm to the target. Intrusive test are typically much more accurate, but obviously they cannot be performed in a productive environment. In contrast, non-intrusive tests cannot determine for sure if the installed service is vulnerable, it can only determine if it might be vulnerable [11, p. 88].

- Mapping the application is done after the attacker during the network scanning, has found a system that hosts a web application. It identifies the vulnerabilities. Vulnerabilities in web applications are very common. Often these applications security layer holes could be used to circumvent all the perimeter defences. The primary step in the process of attacking the application is to gather some key information about it. A few activities of web application mapping overview are described below [55, Ch. 4]:

  - Enumerating Content and Functionality, it is a basic approach by walking through the application starting from the main initial page, following every link and navigating through all multi-stage functions. However, they are advance techniques that can employ simple browsing, such as, web spidering and user-directed spidering. Various tools exist for automated spidering of web sites.

  - Discovering Hidden Content, it is very common for applications to contain content and functionality which is not directly linked or reachable from the main visible content. A common example of this is functionality that has been implemented for testing or debugging purposes and has never been removed. There are countless other cases in which interesting content and functionality may exist, for instance the backup copies of live files, log files, etc. Another approach is by performing brute-force techniques, as well as the use of public information or leverage the web server.

  - Application Pages and Functional Paths, it has inherited the application from the pre-application days, in which web servers functioned as repositories of static information, by using retrieved URLs that were effectively file names.

  - Discovering Hidden Parameters, it is a variation on the situation where an application uses request parameters to specify which function should be performed increases when other parameters are used to control the application's logic in significant ways. For example, an application may behave differently if the parameter *debug=true* is added to the query string of any URL or allow the user to bypass certain access controls.

  - Analysing the Application, is by analysing the application's functionality, behaviour, and technologies employed, in order to identify the key attack surfaces that it exposes, and begin formulating an approach to probing the application for exploitable vulnerabilities.

  - Identifying Entry Points for User Input, is by capturing user input.
  - Identifying Server-Side Technologies and Functionality, identifying by fingerprinting the technologies employed on the server via various clues and indicators. For example: banner grabbing, HTTP fingerprinting, file extensions, directory names, session tokens and third-party code components. On the other hand, it is possible to infer server-side functionality and structure, or make a guess, by observing clues that the application discloses to the client. For instance: dissecting requests and extrapolating application behaviour.
  - Mapping the Attack Surface, it is a final stage of the mapping process and it is to identify the various attacked surfaces exposed by the application, and the potential vulnerabilities that are commonly associated with each one. Such as: client-side validation, database interaction - SQL injection, file uploading and downloading, multi-stage login, access controls, error messages and so forth.

4.1.3 Gaining Access

The third step after the attacker has finished scanning the target network, vulnerabilities etc. is to gain access in the target system. There are two particular approaches to gaining access depending on the requirements. The first is to gain access by using application and operating systems attacks [51, ch. 7]. And the second involves, gaining access by using network attacks [51, ch. 8].

For the attacker to be able to gain access using application and operating systems attacks several sophisticated highly pragmatic approaches should be taken into consideration. These are noted below in the overview description [51, ch. 7]:

- Script Kiddies, is an exploit program that craft very specific packets designed to make a vulnerable program execute commands, cough up unauthorized data, or even perform a DoS attack.
- Buffer Overflow Exploits, is a phase when the attacker gains access to and has a significant degree of control over a vulnerable machine. For instance, the operating system or application. It entirely gives control to the attacker to execute commands, steal important and valuable files or even delete. There are many ways of performing buffer overflow exploitation; one of most common is stack-based buffer overflow.
- Password Attacks, are well known attacks and they are often the weakest link of the securing system as well. It is done by guessing passwords into the targeted machine, where after the good match the attacker can gain entire access of the machine, depending on the privilege of the targeted user.

- Web Application Attack, the attacker can conduct access into the account and harvest and attack sessions with tracking mechanisms, SQL injection, and many other techniques which will deliver to and provide the attacker with extremely useful information in order to be able to successfully gain access.

- Exploiting Browser Flaw, is almost the same as buffer overflow exploits, where the attacker in this case concentrates only on the possible vulnerabilities of the browser. By exploiting the browser the attacker can execute any system command or even open a third party application so as to collect further information.

Secondly for gaining access using network attacks we expose few techniques and tools that can be used in both wired and wireless attacks, including sniffing, spoofing, session hijacking and network tool called Netcat[1]. The list below presents the overview [51, ch. 8]:

- Sniffing, is a program that gathers traffic from the local network, and it is useful both for attackers looking to swipe data as well as network administrators trying to troubleshoot problems. In fact, by sniffing attacker can read data passing through real time, or store data in a file for access at a later time. For instance, the attacker can capture the user IDs and passwords, DNS queries and responses, sensitive e-mail messages, FTP password, and much other useful information. There are different types of sniffing, such as, sniffing through hubs: passive sniffing and active sniffing; dsniff: sniffing cornucopia such as, HTTPS and SSH, sniffing and spoofing DNS, foiling switches with port stealing, etc.

- IP Address spoofing, another fundamental component of numerous attacks involves changing or disguising the source IP address of a system, or in other words IP address spoofing. Spoofing will help the attackers if they do not want their actions to be traced back, and undermine various applications. Spoofing can be done by predicting TCP sequence numbers to attack and through source routing.

- Session Hijacking, is a combination of sniffing and spoofing, these tools can be particularly nasty. When a user has an established interactive login session with a machine, using either telnet, SSH, FTP, etc. the attacker can use a session hijacking tool to steal the session from the user. Hijacking can be conducted by host-based session hijacking, hacking with a tool called Ettercap[2] and attacking wireless access points.

[1] Netcat: `http://netcat.sourceforge.net/`, last checked 17.04.2012

[2] Ettercap: `http://ettercap.sourceforge.net/`, last checked 17.04.2012

4.1.4 Maintaining and Expanding Access

After the attacker, has successfully penetrated the defences and gained access to the targeted system, their aim is to maintain and expand that access. The next logical goal of the adversary would be to consolidate the access and to compromise the resources. To achieve these goals, the attacker should utilize techniques based on malicious software such as trojan horses, backdoors, bots, and rootkits. Alternatively, the attacker can add new user accounts to the system and configure remote access to the system.

However, to be able to understand the above tactics of exploitation, a sound understanding of tools is essential. Thereby, we annotated the most common known techniques [51, ch. 9]:

- Trojan Horses, is a software that consists of programs that appear and begin to hide malicious activities. In other word, they make the user run the Trojan horse program by making it appear attractive and disguising. In fact, the main purpose is to crash systems or destroy data, or on the other hand, to allow the attacker to steal data or to remotely control systems.
- Backdoors, is a software that literally allows the attacker by the employing the method of backdoors. Thus, bypassing the normal system security control that act as the front door, the attacker can access the system without using the passwords, encryption, and account structure associated with normal users of the machine.
- Rootkits or user-mode rootkits, are more insidious than the previous techniques. They raise the ante by altering or replacing existing operating system software. They do not run as a foreign application. The user-mode rootkits modify critical operating system executables or libraries to let an attacker have backdoor access and hide on the system.

Due to the fact that the attacker has collected, gained and maintained or expanded access to the targeted system, now it is a time to cover the tracks. The next section explains the techniques and possible tools for covering the tracks and remaining in a system as a legitimate user.

4.1.5 Covering Tracks

Concluding on the current attacking phases, we introduce the participants to the final phase and action that an attacker may consider. Most the attackers prefer a quiet and secret access to avoid detection. Thus, the perpetrator will try to cover and hide the tracks and in the end the final step will be to destroy as much evidence about the intrusion as possible.

There are a few techniques that the perpetrator can use, such as:

- Hiding evidence by altering the event logs, is by avoiding detection by system, network, and especially from security administrators, the attackers alter the logs of their targeted system. Even though some of the techniques that we have mentioned previously are incredibly powerful and allow to mask the activities, in the end they can often be traced, due to the installation process on behalf of event logs. The best known way of hiding the activities and the actions is to remove the event logs of the targeted system to make sure that the consensuses will not follow. Since there are different operating systems, a variety of actions are needed.
- Diffuse access of files and directories, this is another approach used by attackers, the main idea is to create “hidden” directories and files to store various attack tools loaded on the system, save sniffed passwords, and other information belonging to the assaulter. And of course, in different operating systems diverse approaches should be considered.
- Covering Channels - Tunnelling and proxy, is final step, after the intruder has diffused the logs and files that aim to clean up their tracks, next is the avoidance of detection, by utilizing stealth mechanism to communicate with backdoor systems across the network. Such communication mechanisms are covert channels for instance tunnelling and using proxy.

Anyhow, by illustrating the framework of the attacking phases, the activities will aim to give the participants a better understanding and a clearer view, in a step-by-step manner, and then present solutions. By letting them know for instance how the attacker of the system collects useful information; how they gain access and maintain it, and finally how they cover their tracks and steps. In this module, the following units demonstrate numerous scenarios of attacking tactics and activities mentioned above, and the recommended defence against them.

4.2 Network Scanning Attacks

Network scanning attack is a mode of operations for gathering information about the network by discovering live hosts, open ports and services that are listed on those ports, determining the operating system fingerprint and identifying possible vulnerabilities. It can be used by the system administrators, network engineers, audits and security specialists for network asset management, security auditing and compliance checking, as well as by the intruders to discover interesting targets to the system.

Usually, network scanning begins with the host discovery to identify which IP addresses have alive system behind them. Secondly, purpose of port scanning is to identify the state of target’s TCP and UDP ports. After identifying the TCP and UDP ports, the next logical question would be: what services are listening, what are the specific versions of the applications and what operating system the target is running. In the end, the answers to these questions are useful to determining if the host is vulnerable to specific exploits and flaws or identify unauthorized or dangerous devices in the network.

We describe each of these operation types in the following units, in addition to the countermeasures and conclude with further improvements.

4.2.1 Host Discovery and Port Scanning

To be able to build an inventory of accessible systems, the best way is to ping all possible addresses in the target network to determine which ones are alive hosts. By sending ping, in other words ICMP Echo Request packets to every possible address in the network will result within a return message. If a reply comes back, that address has an active, alive machine. For this purpose there are automated tools to sweep the entire target address space looking for live hosts. Such as, nmap[3], ping scan, etc.

However, often some hosts have configured their firewalls to block some of the ICMP traffic where in the end is not always reliable. Other popular methods of discovering alive hosts is by port scanning, such as TCP SYN ping, TCP ACK ping and UDP ping. Moreover, remote ports can be classified as open, closed, filtered, unfiltered, etc. Alternatively is to send a TCP packet to a port that is commonly open, such as TCP port 80, web server. If the port is open, the system at the target address responds with a SYN-ACK packet, indicating that there is a machine at that address. Or, by sending a UDP packet to an unusual port, if the port is closed, many machines will respond with an ICMP Port Unreachable message, another good indicator that a system is located at the given target address.

As a result, we illustrate three methods of identifying whether a host is alive and open ports, by: ICMP pings, TCP packets to potentially open ports, and UDP packets to likely closed ports.

4.2.2 Service, Application and OS Version Detection

After identifying all open ports in the target, the next approach is to identify what services are listed on those ports, what the specific versions of the application are and what operating system the target is running.

For this purpose network scanners are capable of sending specific service probes to the target ports. The responses to the probe are compared to the database containing details about thousands of well-known services. Such as, stack fingerprinting can draw inferences on operating system or application version from observable packet signature and network behaviour, and software or service versions may be identified via banner grabbing or application fingerprinting.

[3] Nmap: `http://nmap.org/`, last checked 17.04.2012

Stack fingerprinting refers to a series of techniques that are used to determine the operating system running on a target host by examining characteristics of the TCP/IP stack implementation. By probing the stack for these characteristics and aggregating various stack *tests*, it is possible for a port scanning tool to differentiate one operating system from another [67, p. 114].

Determining the operating system and application version of a host is extremely useful for further action, even in instances where a specific application port, such as TCP/80, TCP/53 is being targeted. By determining the underlying operation system or service can assist in adjusting the exploit code to accommodate the operating system, application or service.

4.2.3 Vulnerability Scanning

Since we identify a series of accessible network ports for a set of target systems and any associated application information, the next step is usually to embark on the process of identifying specific operating system and application vulnerabilities. For this purpose we will use vulnerability scanning method.

Vulnerability scanning entails using a vulnerability scanning application to run a vulnerability scan against a set of targeted IPs. Vulnerability scanning can quickly harvest a number of relevant IP, service, operating system, and application vulnerabilities but can sometimes utilize significant bandwidth in many network environments [67, p. 115].

Objectives of vulnerability scanning are to harvest a large number of vulnerabilities in a single pass against the targeted system. They might range from application code weaknesses to account management and operating system and applications configuration issues. In fact, vulnerability scanners have been favoured by system administrators to conduct penetration testing.

Features of vulnerability scanners are noted below:

- Port scanning facilities.
- Operating system and application profiling.
- Operating system and application vulnerability identification.

By identifying the vulnerabilities of operating system, service and applications the intruder can gain access to the targeted machine and can behave offensively and control the system.

4.2.4 Scanning Countermeasures

After we have illustrated the networking scanning methods, next we demonstrate to the participants, what approaches should be considered in the defence against those attacking methods.

Primarily, the methods and tools can be conducted into the network environment with the purpose of understanding alive hosts, open ports and in addition the vulnerabilities in the system, services and applications.

To be able to pursue a better defence line and countermeasures, the following approach should be taken into consideration:

- Blocking ICMP messages by using firewalls and the packet filtering capabilities of routers.
- Close all unused ports such as FTP, telnet, mail or web server.
- Stop unneeded services and delete the program files associated with them.
- Find the open ports before the intruder does.
- Use the provided tools, such as *nmap*, scan each port and protocols to identify the vulnerabilities.
- Use more intelligent filtering device on the network, for instance a stateful filter or a proxy-based firewall against advance scanning.
- Determine the firewall filter rules.
- Keep the system patched to defend against the vulnerabilities.

All in all, these are best practices for securing countermeasures against network scanning. However, another approach is to run the tools against one's own network, which will help to determine the above issues. Additionally, vulnerability scanning tools are extremely useful, yet they have their limitation, such as they can only check for vulnerabilities that they know about. They cannot detect vulnerabilities that they do not understand.

As a result, we illustrate to the participants to understand how attackers armed with information from a detailed network scan, can compromise systems on the target network and how to defend against these attacks.

4.2.5 Further Improvement

Network scanning is extremely important, valuable and essential for system administrators, auditors and security specialists. It includes not only one attacking phase, but it is an important tool for reconnaissance, scanning and of course gaining access.e We have covered only the most well-known attacking strategies of scanning over the network and the countermeasures. In the future we should prepare types of attacks covering more advanced techniques and advanced countermeasures. However, we do not plan to drop the above types and the topic. Furthermore, many participants still find it interesting and useful. The following items should be considered to improve the curriculum of network scanning by adding the types of attacks:

- Denial-of-Service Attacks. Most of DoS attacks are merely bothersome. In many cases they crash the system, where further action is needed from system administrators or users to restart the targeted machine.
- Vulnerability methods, to be more precise we can separate the vulnerability scanning into the following segments:
  - Manual vulnerability probing. It entails manual connection to ports using *telnet* or *netcat* to identify operating systems or application banners and the use of a security site to identify exploitable vulnerabilities in specific software version.
  - Traffic monitoring. Conducted if the attacker has access to a sniffer, protocol analyser, or network Intrusion Detection System (IDS) on an appropriate network segment, to capture the operating system and application information from active network sessions.
- Finding Wireless Access Points. An incredibly popular scanning technique involves searching a target organization for accessible and unsecured Wireless Local Area Networks (WLANs). The intruder can choose from a wide variety of tools to perform this attack, but each tool tends to centre around one of three specific techniques for finding wireless access points and determining their ESSID. Those techniques include the following: active scanning, passive scanning and forcing de-authentication.
- IPS and IDS evasion. Authorized personnel can usually access the network they need to scan behind the intrusion systems and it is useful to test the techniques that make the detection and prevention of the malicious traffic more difficult. Indeed the intruders will use those methods! Since intrusion systems are constantly evolving we need, firstly to identify the evasion methods that are not relevant any more.
- Implementation of testing techniques behind stateless firewalls.
- Consider IPv6 implications to network scanning.

Also we should take into account advanced techniques for countermeasures. For instance the following:

- Email security, like Sender Policy Framework (SPF) and Domain Keys Identified Email (DKIM) implementation or client side e-mail security for instance, Pretty Good Privacy (PGP) or Secure/Multipurpose Internet Mail Extensions (S/MIME) and additional spam countermeasures.
- DNS security, such as Domain Name System Security Extensions (DNSEC).
- Wireless security.

4.3 Password Attacks

Passwords are most commonly used tool for computer security, for instance, to login into the system and for e-mail access. Unfortunately, though having a central role in security, they are actually the weakest links in the security of the system. By simple guessing of a password can retrieve and provide access to the system and the intruder can then access very sensitive information.

In fact, every user has at least one password, and many users dozens of passwords. Therefore, the intruder will use methods and observe the possibilities on how to gain access to the targeted system. However, in this section we will annotate only the most common types of password cracking methods, although there are enormous types of methods. Applications and tools that whose aim is to guess the passwords. And in addition what countermeasures should be applied for better protection. We conclude with further improvement.

4.3.1 Types of Password Attacks

Depending on how an attacker tries to crack passwords, password hacking attacks can be classified as follows [26, ch. 4]:

- Passive Online Attack, is when the attacker does not contact the authorizing party to steal the password, in other words he attempts password hacking but without communicating with the victim or victim's account. Types of passive online attacks include wire sniffing, Man in the Middle attack and reply attack.

- Active Online Attack, this type of attack can be directly termed as password guessing. Whereby the attacker tries a list of passwords one by one against the user account to crack the password.

- Offline Attack, are performed from a location other than the actual machine where the password resides or is used. Offline attacks requires physical access to the targeted machine which stores the password file. In this case, the attacker copies the password file and then tries to break the password on his own system. Offline attacks include, dictionary attacks, hybrid attacks, brute-force attack, precomputed hash attacks, syllable attacks, rule based attacks and rainbow table attacks.

- Non Technical Attacks, it does not require any technical knowledge hence the term non-technical attacks. This kind of attack may include, social engineering, shoulder surfing, keyboard sniffing and wheelie bin diving.

Tools that can help in performing the above password guessing are, Cain & Able[4], John the Ripper[5], NCrack[6], L0phtcrack[7] and others. Each of these applications can perform one or more methods of password cracking. Some of them have advantages and disadvantages.

In the end, with the above list of password cracking methods and types, we illustrate the basics, while on the other hand we provide the participants with a list of tools that are extremely useful for a future action of password cracking.

4.3.2 Password Countermeasures

After the participants have received the basics of understanding password cracking techniques and methods, we then illustrate to the participants how to defend against those techniques and different methods of cracking passwords.

There are two options of defending against password guessing and password attacks. Both smart cards and biometrics add a layer of security to the insecurity that's inherent when users create their own passwords [26, ch. 4].

Moreover, we demonstrate another awareness approach for the organizations such as, creating a strong password policy, for instance, to specify a minimum length and prohibiting the use of dictionary terms. Meanwhile, in complying with password policy, users must be aware of the security issues associated with weak passwords and be trained to create memorable, yet difficult to guess passwords. Or another approach can be the use of password filtering software.which will help to make sure users do not select weak passwords. For example in Windows operating systems StrongPass[8], alternatively for Unix systems passwdqc[9] [51, ch. 7].

On the other hand a good practice for system administrators is to monitor and check the logs into the system or other defending tools, such as, setting the firewall or IDS system rules to be able to identify the password attacks.

4.3.3 Further Improvement

Although we have mentioned the types of password attacks and their countermeasures, it can be extremely favourable if we expand the list and provide more details of possible types and techniques of password attacking, for instance, one of the most common and straightforward used passive attacks are Man in The Middle Attack

[4] Cain & Able: http://www.oxid.it/cain.html, last checked 17.04.2012

[5] John the Ripper: http://www.openwall.com/john/, last checked 17.04.2012

[6] NCrack: http://nmap.org/ncrack/, last checked 17.04.2012

[7] L0phtcrack: http://www.l0phtcrack.com/, last checked 17.04.2012

[8] StrongPass: http://www.ntsecurity.nu/toolbox/strongpass/, last checked 17.04.2012

[9] passwdqc: http://www.openwall.com/passwdqc/, last checked 17.04.2012

and brute-force attack, even dictionary attack and moreover we can, by expand and deliver in further detail g the usage of password cracking tools.

For instance, simple illustration is when two parties are communicating; the man-in-the-middle attack takes place if a third party intercepts the communication between the two parties. Whereby, the third party may alter the data or simple eavesdrop. To be able to complete this task, the man-in-the-middle has to sniff from both sides of the connection simultaneously. For instance, this kind of attack is found in telnet and wireless technologies. This attack is not easy to implement, due to the TCP sequence numbers and speed. An alternative illustration is for instance, a replay attack, when the packets are captured using a sniffer. After the information is extracted, the packets are placed back on the network. This type of attack can be used to replay bank transactions or other type of data transfers.

Also by demonstrating how to gain access to encrypted hard drives, partitions or files will be extremely intriguing and profitable for the participants to perform these techniques of password cracking.

However, by demonstrating the password attack to the participants, they will have a better understanding of performance and implementation.

4.4 Exploitation

In this section of advance curriculum we emphasize the basics catalogue exploitations of vulnerabilities in the targeted system, likelihood, operating system, services and application vulnerabilities. This approach mainly involves interaction with the system in unexpected and malicious ways, and exploiting anomalies in the operating system, services and application's behaviour in order to extract valuable information.

First of all, we discuss the basics of memory segmentation and buffer overflow and the exploitation frameworks. Then, we supply the participants with possible countermeasures and closing by the further improvement of this module.

4.4.1 Memory Segmentation

To have a better understanding of the essence of buffer overflow vulnerabilities, we firstly have to consider the segmentation of process memory based on Jon Erickson's description [20, ch. 0x270]. Compiled programs memory is divided into five segments: text, data, block storage segment, heap, and stack. Whereby, each segment represents a special portion of memory that is set aside for a certain purpose.

Text segment or in other words code segment contains the assembled machine language instructions of the program. The data and block storage segment are used to store global and static program variables. These segments are writeable and have a fixed size. Furthermore, heap segment is a segment directly controlled by the programmer. It is not of a fixed size, and it can grow larger or smaller as needed with the help of allocator and deallocator algorithms. The stack segment also has variable size and it used as a temporary scratch pad to store local function variables and context during function calls. When a program calls a function, that function will have its own set of password variables, and the function code will be at a different memory location in the text or code segment. Common data elements placed in the stack, include the parameters passed to the function, functions local variables, saved registry information, and return address. The return address is a crucial element in the context of stack based overflows. It is used to remember the address where the program should jump when the function finishes execution and returns. All the information that is stored in a stack is collectively called a stack frame and it contains a lot.

4.4.2 Buffer Overflow

Buffer is an element of physical memory storage used to temporarily hold data while it is being shifted from one place to another. In addition, buffer overflow or buffer overrun condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. The buffer is a sequential section of memory allocated to contain anything from character string to an array of integers. For example, if the programmer wants to put ten bytes of data into a buffer that had only been allocated seven bytes of space, that type of action is allowed, although it will most likely cause the program to crash.

Moreover, programming languages such as C or C++ do not perform bounds checking to prevent writing past the end of a buffer. Thereby the programming has to perform these checks themselves in the code. For instance, in languages C and C++, data can overflow both stack and the heap segmentations. Likewise, they may overwrite security critical data and in worst case scenarios allow the attacker to remotely execute arbitrary code on the vulnerable system.

However, heap based overflows are generally more difficult to exploit than stack overflows. For instance, first the attacker has to figure out some security critical variables to be filled with the desired value. Secondly, the attacker has to find a buffer that can overflow in such a way that it overwrites the target variable. This generally means the buffer needs to have a lower memory address than the target variable [63]. Thus, heap overflows are common and can cause real security problems.

In addition, stack based overflows have been more widely exploited and are better understood than other buffer overflow methods. They are somewhat easier to implement because there is always something critical to overwrite on the stack - return address. Typical stack based overflow attacks consist of the following steps [63]:

1. Find a buffer allocated in stack that can be overflowed and that allows to overwrite the return address in stack frame.
2. Place some hostile code in memory to which the program can jump when the function returns. Usually, code that gives the attacker remote shell access is used as this hostile code. It is therefore called a a shellcode.
3. Write over the return address on the stack with a value that causes the program to jump to the hostile code.

Finally, to be able to craft a working buffer overflow exploit is usually very hard work and requires a good knowledge in programming, a considerable amount of time, and of course talent.

4.4.3 Exploitation Frameworks

Today, both the attackers and penetration testers increasingly rely on powerful exploitation frameworks to launch their attacks. Exploit frameworks include an arsenal of different exploits and an arsenal of different payloads, by offering a different effects that suit the attacker's intention on the attacking system. For instance to compromise an unpatched system, script-kiddie is enough. Yet for more different payloads free tools like Metasploit[10] or commercial tools like CORE IMPACT[11] and Immunity Canvas[12].

Exploitation frameworks are developed to reduce the complexity and to increase the speed of developing new exploits. They contain enormous amounts of ready-made modules. However, many of the tools are abused by the attackers, on the other hand, the main goal and purpose of exploitation frameworks is to aid the penetration testers, vulnerability and security researchers.

4.4.4 Exploitation Countermeasures

There are a variety of ways to protect against the exploitation attacks. For instance to defence against buffer overflow attacks, should be taken into consideration of applying security patches in a timely manner, filtering incoming and outgoing traffic, moreover, configuring systems so that their stacks cannot be used to store executable code. Another approach is when software developers can help with stopping buffer overflows by utilizing automated code checking and compile time stack protection tools.

[10] Metasploit: `http://www.metasploit.com/`, last checked 17.04.2012

[11] CORE IMPACT: `http://www.coresecurity.com/content/core-impact-overview`, last checked 17.04.2012

[12] Immunity Canvas: `http://www.immunitysec.com/products-canvas.shtml`, last checked 17.04.2012

Finally, by using the exploitation framework against one's own system to identify the vulnerabilities, will help and prevail to reduce the exploitation in the system, and alternatively to identify if the system is unpatched by applying the script-kiddie.

4.4.5 Further Improvement

The under mentioned ideas is only a small subset of potential future developments:

- For instance to setup an exercise for participants that could exploit browser flaws will be very handy.
- There should be more advanced examples on buffer overflow attacks. One approach is to write a simple C/C++ network service with buffer overflow vulnerability, and run it on an environment without stack protection mechanisms such as non-executable or randomized stack, canaries. Then the source code is shared with the participants and this gives them opportunity to write their own exploit against this custom service.
- Demonstration of some available script kiddies against targeted system or to make the participants to write their own script kiddie against a public web site, for instance.

4.5 Web Application Attacks

The last type of attacks that we consider is mainly web application attacks, although they could be combined with network or operating system attacks. Web applications remain the third most common vector. The inherent need for many web applications to be Internet visible makes them a logical target; the potential to use them as an entry point into a corporate database makes them an attractive one. In 2012, the Verizon RISK Team reports that they are 54% breaches reported and successful 29% of records attack vector [57, p. 32]. Consequently, they are actually primary target to the intruders. Most of the web applications are connected within the organization database server to be able to produce the results of queries.

However, to write a powerful web application in a short period of time is achievable even for a novice programmer and it requires a considerable amount of knowledge, skills and time. It is therefore, the attackers always attempt to go with an easier attacking approach like cross site scripting, SQL injection or cross site request forgery. On the other hand protection from an attack is complicated.

Additionally, we provide the participant with a list of useful tools that will aim for web testing application security. Although there are plenty of tools, we concentrate only on the most common ones, like Burp Proxy[13], Webscarab[14], Canoo WebTest[15] and many others. The initial idea for these tools is to test web applications for vulnerabilities and exploitation for security researchers, yet they are an opportunity to the attackers too.

Several web application methodological types of attacks are described in the following sections.

4.5.1 Session Management and Path Traversal Attacks

We have separated the following section into two mini-sections.

Path Traversal

Sometimes, web applications have to read from or write to a file system on the basis of parameters supplied by the user requests. If these operations are carried out in an unsafe manner, the attacker can read sensitive data, such as password and application logs, and he can overwrite the configuration files and software binaries. Another scenario is a case where the vulnerability enables the attacker to completely compromise both the application and the underlying operating system. Those are known as path traversal vulnerabilities.

One of the simplest examples of illustrating path traversal is by using the "dot-dot-slash" sequence, in other words using "../" in URL, it enables the attacker to read or write data including application source code, configuration and critical files. To better understanding, consider the following example:

http://.../images/logo.png

The server can process this request by extracting the value of file parameter, append this value to the prefix like /var/www/client1/images/, and finally open the file with this name and return it to the client.

At this point the vulnerability arises because of placing path traversal sequences into the file name in order to backtrack up from the image directory and to access files from anywhere on the server. The typical attack would look like this:

http://.../images/../../../../etc/passwd

In the above example the attack has gained access to a file named *passwd* that contains a list of the system accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc.

[13] Burp Proxy: `http://www.portswigger.net/burp/proxy.html`, last checked 17.04.2012

[14] Webscarab: `https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project`, last checked 17.04.2012

[15] Canoo WebTest: `http://webtest.canoo.com/webtest/manual/WebTestHome.html`, last checked 17.04.2012

Because of the extreme importance of path traversal vulnerability, we provide the participants with several different examples in the curriculum, for better understanding.

Session Management Attack

Session management is an essential and crucial security component in majority of web applications. In fact, HTTP protocol is stateless and is based on a simple request-response model. Each pair of messages represents several transactions. Moreover, the protocol contains no mechanism for linking together the series of requests made by the user and distinguishing these from all of the other requests received by the web server. Therefore, the application has to use methods to recognize each user's session, and the most common way is by issuing each user a unique token. On every subsequent request to the application, the user resubmits this token, enabling the application to determine, which earlier request the current request related to. The token can be sent in the HTTP header as a cookie, placed in other parts of the header, specified in the URL or even in the body of the HTTP request.

Moreover, the primary goal for the attacker is to gain unauthorized access to the web application by hijacking authenticated user's session. Basically, the intruder needs to predict or steal a valid user's session token. The typical methods for hijacking include the following [30, p. 56]:

- Exploiting weaknesses in the generation of session tokens. Sometimes the developers use custom schemes for generating session tokens. This has occasionally resulted in creation of tokens that are not random and that could be predicted.
- Exploiting weaknesses in the handling of session tokens. Session tokens can also be acquired by sniffing traffic on the network. The identifiers can be disclosed in logs, if they are passed in unsafe manner like in URLs: user's browser logs, web server logs, Internet Service Provider (ISP) or corporate web proxy logs, HTTP Referrer logs in servers that are visited by following off-site links.
- Client-side attacks: cross site scripting (Sec. 4.5.4), Trojans.

4.5.2 Code Injection

Although there are many types of code injection attacks like different environments and languages, still this class of attacks depends on inserting malicious code into the application and after words is interpreted and executed. In details, the application usually receives user-supplied data, where it manipulates and acts upon it. In some situations the attacker can supply crafted input that breaks up the data context and supplies syntax to interpret it as program instructions. The cause of vulnerabilities exploited by code injection is appropriate input and output validation.

We have illustrated to the participants only a few code injection types against a few technologies. SQL injection receives more coverage in a next section (Sec. 4.5.4). We only note the OS Command injection and File inclusion in the following lines.

OS Command Injection

This occurs when the attacker attempts to execute system level commands through a vulnerable application. For instance, this can be achieved by passing the command-line command in the URL or into the input form. Consider the following PHP example:

```
   <?php
        $error = system(’cat’.$_GET[’pagetag’], $tags);
        echo $error;
?>
```

For this kind of code, the possible way of attacking to demonstrate is by using live HTTP header or using a method GET to make the following petition:

```
http:/../index.php?pagetag=test;ls /home/
```

With the above example, we have executed the command ls for a home directory, that will supply the attacker with a list of users’ home directory. Afterwards the attacker can use the above code injection to execute other commands on the server.

This is only one simple and easy way of demonstrating the code injection, on the other hand in the curriculum of participants we have illustrated more examples of code OS injection.

File Inclusion

File inclusion or in other words a remote file inclusion is a type of vulnerability most often found on web applications. It allows the attackers to include remote files, usually through a script on the web server. This kind of vulnerability occurs due to the use of user-supplied input without proper validation.

A good example of the vulnerability is provided below in a PHP script:

```
   <?php
        $color = ’green’;
        if (isset ($_GET[’COLOR’]))
        $color = $_GET[’COLOR’];
        include ($color . ’.php’);
?>
   <form method=”get”>
        <select name=”COLOR”>
             <option value=”red”>red</option>
             <option value=”green”>green</option>
        <select>
          <input type ="submit">
    </form>
```

The primary intention of the developer is only a green.php and red.php to use as options. But on the other hand, anyone can actually easily insert arbitrary value in COLOR, and it is possible to inject code from files:

- */index.php?COLOR=http://www.hackerbox.net/r57shell1.40.txt?* - Injects a remotely hosted file containing a malicious code.
- */index.php?COLOR=C:\\ftp\\upload\\exploits* - Executes code from an already uploaded file called exploits.php, which is a local file inclusion vulnerability.
- */index.php?COLOR=C:\\notes.txt%00* - It is an example of using NUL meta character to remove the .php suffix, which allows the attacker to access files other than .php.
- */index.php?=COLOR=/etc/passwd%00* - Allows an attacker to read the content of the passwd file on the UNIX system directory (see Sec. 4.5.1 Path Traversal).

The above examples demonstrate to the participants an attack that can occur through the file inclusion and remote file inclusion. Although by default the PHP5 does not allow to include remote files, yet we have demonstrated solutions by uploading the application or file into the system, whereby the attacker can execute the shell to the server and then include it as a local file.

4.5.3 SQL Injection

Almost every web application employs a database to store different types of information in order to operate. It is therefore, the most common and most well understood level attack. If it is done in an unsafe way the application may be vulnerable to SQL injection. SQL injection can enable an anonymous attacker to read and modify all data stored within the database and even take full control of the server on which the database is running. Moreover, the fundamentals of SQL injection are common to the majority of database platforms. However, there are many significant differences in the details.

The latest report of Verizon [57, p. 67] states that 60% of SQL injection attacks in the 2011 dataset were single-event incident. Where, single-event incidents are often over and done in a matter of second or even milliseconds.

However, in the big spectrum of SQL injections, we have concentrated our efforts to deliver to the participants only a fraction of different aspects on the SQL injection.

Injection into string parameter

The classic example of SQL injection considers bypassing a form based login. Consider the authentication form of a web application works as follows. Form: the username and password specified in user input, the following SQL query will be arranged:

```
SELECT * FROM ‘usersdata‘
WHERE username =’$username’ AND password=’$password’
```

If this request returns at least one row, the login succeeds. Second, suppose the application allows to insert string as the username, such as:

```
&username = “bob’ OR 1=1 – “
```

The following query is requested from the database:

```
SELECT * FROM ‘usersdata‘
WHERE username = ’bob’ OR 1=1 – ’ AND password=’$password’
```

In fact, we note that, the double hyphen tells the SQL query interpreter that the remainder of the line is a comment and should be ignored. The following query will return all rows from the usersdata table and the password will be not checked at all.

Injecting into numeric variable

Almost any good skilled web application developer is primarily considering the countermeasures against SQL injection to escape and filter out the dangerous metacharacters like single quotes or hyphens. In fact, this approach can be very difficult in ensuring security, indeed one has to take into account numerous special cases. For example, numeric user-supplied data is often not encapsulated within single quotation marks. Take into account the following SQL statement:

```
SELECT * FROM employees
WHERE employees_number =$employees and pin =$pin
```

The attacker is able to exploit this query by injecting a sting so that the statement becomes:

```
SELECT * FROM employees
WHERE employees_number=111 OR 1=1 # AND pin=0
```

Also hash symbols can be used in MySQL, for instance, to denote the beginning of a comment. It therefore, escapes or rejects single quotes and hyphens fail in this particular case.

The UNION operator

Another more advance SQL injection is by using the UNION operator. In other words, it allows the attacker to combine information from different number of tables. Moreover, the union operator is possible to execute SQL cross-table queries. Basically it allows the poisoning of a query to return records from another table. The following example illustrates this attack:

```
SELECT author, title, year FROM ‘books‘
WHERE publisher=’$publisher’
```

Consider that the value $publisher is under control of the attacker. Next the attacker can cause the following query to be requested from the database:

```
SELECT author, title, year FROM ‘books‘
WHERE publisher=’something’
UNION SELECT user,password,2
FROM usersdata.user –’
```

From the above example, the poison will result in the rows of users that are stored into the usersdata table.

Blind SQL injection

Normal SQL injection allows the attacker to execute of the SQL injection code to return within the web response. However the attacker is also able to force the application to reveal the SQL statement, or at least part of the statement, that is made by the web application to the back-end database. This approach is done by forcing the web application to produce an error that discloses SQL information. All in all this kind of approach can be conducted through blind SQL injection.

Blind SQL injection does not reveal any part of the SQL statement or SQL results. However, it could be possible to use injected query to conditionally trigger some detectable behaviour by the database. This can simply be done by a different page or message returned on successful SQL injection. Another option is by using timed attacks, where the web server requests a pause of a number of seconds before returning the page. The data can be dumped by asking several true or false questions [28, p. 385].

4.5.4 Cross Site Scripting

After we have demonstrated to the participants how to attack directly by targeting the server side application, next we are going to note the different types of techniques used to cause trouble. By applying Cross-site scripting (XSS) and cross-site request forgery (CSRF, Sec. 4.5.5) attacks target the other users of the application, although the vulnerabilities still exist within the server side.

Actually, XSS currently is the second most prevalent security vulnerability in web applications for OWASP top 10 Application Security Risks - 2010[16]. And it is trivial to identify. For instance, they can be used to get control over the entire application.

XSS flaws occur whenever an application takes entrusted data and sends it to the web browser without any validation or encoding the content. They allow the attacker

[16] OWASP Report 2010: `https://www.owasp.org/index.php/Top_10_2010-Main`, last checked 17.04.2012

to inject malicious script in the victim's browser. And this script could be used for hijacking the user session, virtually deface web sites, in addition to capture the contents of the clipboard and port scan local network. Moreover, it can introduce worms in the victim's machine or even cause a denial of service attacks, etc.

However, below in a mini-section we have introduced the participants to several of the most common types of XSS attacks.

Reflected XSS

Reflected XSS occurs when the user supplied input in the HTTP request and it is reflected back into user's browser in the corresponding HTTP response. This approach is common in case of displaying error pages or search results. For instance to consider a web site with a search form, after the user has submitted the search string the following request will be executed:

http://.../search.php?q=SearchString

Suppose that now at the beginning of the returned web page with the search result, the following line is displayed:

Results 1-10 of about 1000 for SearchString (0.21 seconds)

If for instance the application does not validate or sanitize the contents inside SearchString, the attacker could include a link similar to:

http://.../search.php?q=<script>alert('This site has been attacked!')</script>

This script will be executed into the browser after the user has clicked on the link. Indeed, the link firstly has to be delivered to the user. This could be done by e-mail, social networking site, and so forth. And yes, the user has to trust the site, in other words, the link has to be provided within the trusted domain name where the user will trust clicking.

Stored XSS

Stored XSS occurs when data submitted by one user is stored on the targeted server and then displayed to other users without being filtered. Actually, every user that accesses the poisoned link and requests the stored content receives the script, which is in the end executed in the user browser. Store XSS vulnerabilities are common in applications that support interaction between users. For instance, the malicious code could be entered as forum postings, comment fields, user profile parameters, user bookmarks, etc.

Session Hijacking

The best approach of illustrating XSS vulnerabilities is by session hijacking. Take into consideration a web site that is using a cookie based session tokens for authenticating the users. For instance we suppose that the user has already logged into the site, and additionally suppose the web site contains a stored XSS vulnerability and the attacker is able to inject the following java script:

```
<script type=”text/javascript”>

    var cookie=escape(document.cookie);
    document.write(“<img scr=http://.../cookie=”+cookie+”>”);

</script>
```

If the user happens to visit the link where this script is stored, the session token will be sent in the GET request to the attacker server.

4.5.5 Cross Site Request Forgery

Cross site request forgery (CSRF) is an attack that forces a logged-on victim browser to send a forged HTTP request, by including the victim session cookie and additional other automatically included authentication information, to a vulnerable web application. In fact, this allows the attacker to force the victim's browser to generate requests that the vulnerable application thinks that are actually a legitimate requests from the victim.

A list of four serious vulnerabilities in major sites is listed in the research paper from Princeton University [68]. However, CSRF attacks in general work as follows:

- We suppose that the user browser has established an authentication session within trusted site. To conduct this, the user has to log in with username or sometime s a valid e-mail address and password. In internal network the authentication could be also based only on IP addresses.
- By assuming that the attacker has set up a malicious site and is somehow able to trick the victim to visit this site. The attacker could place malicious script or other content to this malicious web site which forces the victim browser to send a request to the trusted site to perform evil action. In fact, the attacker could forge a cross-site request from the malicious site to the trusted site.
- After the user has visited the malicious site, the trusted site sees a valid authentication request coming from victim browser and performs the actions specified in the request. Obviously, we assume that the trusted site does not have any specific countermeasures against CSRF. Thus, the application authenticates the request only relying on the information automatically submitted by the browser, session cookies, HTTP basic authentication credentials, etc.

From the above we can see that CSRF attacks in themselves are simple, but it is not trivial to make it work in a real life. Firstly, the victim has to be tricked to visit the malicious site at the same time when it is logged into the trusted site using simultaneously the same browser. Also, the attacker has to find a form submission at the target site that does something useful for him. This somehow reduces the actual risk.

4.5.6 Web Application Countermeasures

After we have demonstrated to the participants the vulnerabilities and exploitations into the web applications, the countermeasures should be applied. However, in this section we will discuss only the best known practice of counter measuring and bypassing the above attacks into the web applications.

Firstly, for preventing the path traverse, primary is to process URL requests that do not result in a file request for instance if the protection is based on input validation filters, it could be possible to bypass it, because often these filters are poorly designed.

Next, the overall defence-in-depth strategy will be by using strong encryption on all transmissions like cookie based sessions by setting the SSL attribute. Moreover, store only the session ID on the client side, and implement GET variable Referrer Filtering. In addition perform sanity checks to detect session hijacking or use one of the above attacking methods and select a good session identifier. Also it is important to check the vulnerabilities of XSS and CSRF.

Moreover, to be able to defend against the code injection, like file inclusion and command injection problems utilize secure input and output handling, such as: input validation and encoding, selective input inclusion/exclusion, escaping dangerous characters, output encoding, modular shell disassociation from kernel and so on. In addition for SQL injection parametrized SQL queries, also known as prepared statements and sometimes bound variable or bound values should be implemented into the development process of application and coding practice. For advance protection runtime image hash validation or NX bit can be applied.

Nevertheless, this list is actually widely illustrated and displayed into the curriculum for better in depth countermeasures. For each type of web application attack we have provided the participant with the best practice, solutions and hints of how to bypass those attacks.

Finally, as from the above we can see that a lot of information and consideration should be taken into account to be able to secure web applications, however, the best practice shows that the best way to know from what to protect is by knowing how to attack. And therefore, in advance curriculum we have taken into consideration the attacking types by demonstrating real live scenarios and how to be able to secure from them.

4.5.7 Further Improvement

There are many ways of exploiting the web application vulnerabilities. Above we have mentioned only the most common. However, this list can be expanded into the following segments by adding additional web application attacking methods, such as:

- Bypassing the client-side controls. For instance there are two broad ways in which the application may rely upon client-side controls to restrict user input. Firstly, by transmitting data via the client component, using some mechanisms that it is assumed it will prevent the user form modifying that data. Secondly, when gathered data that are entered by the user, may implement measures on the client side that control the content of that data before it is submitted. All this may be achieved using HTML form features, client-side script or thick-client technologies.
- Attacking authentication technologies. For instance by applying brute-forcible login, verbose failure messages, vulnerable transmission of credentials, password change and forgotten functionality, user impersonation functionality and many others.
- Attacking access control, so as to determine access to the application by using different accounts and demonstrating how to create secure countermeasures of access control.
- Understanding and attacking the application logic flaws. Since all applications employ logic in order to deliver their functionality, and by understanding these flaws the participants can probe and attack the application logic.
- Bespoke-ion automation. There are for instance three type of bespoke automation techniques that could employed to attack web application. Such as, enumerating identification, harvesting data and web application fuzzing.
- Demonstration of different employment of injections, like SOAP, XPath, SMTP or LDAP, moreover, injection of different types of SQL server, like Oracle or Microsoft SQL. Additionally, by expanding and demonstrating the different SQL injection types and XSS or CSRF techniques of attacking the targeted system.

4.6 Advanced Persistent Threats

Whether the term Advance Persistent Threats (APT) is used in the context of cyber attacks (or cyber security) each component of the term is relevant [34].

Advanced is when the hacker has the ability to evade detection and the capability to gain and maintain access to well-protected networks and sensitive information contained within them. The hacker is generally adaptive and well-resourced. *Persistent* is when the threat makes it difficult to prevent access to computer network and, once the threat actor has successfully gained access to a network, and it is very difficult to remove. And in the end, *threat* is when the hacker has not only the intent but also the capability to gain access to sensitive information stored electronically.

Several significant attacks likely attributable to APTs can be illustrated, from recent to older, such as [34]:

- May/June 2011 – International Monetary Fund, compromised the accessibility to internal systems and files.
- 26 May 2011 – Northrop Grumman, shutting down remote access to its network without warning and conducting an organization wide password reset, raising speculation that it had also been targeted using information stolen from RSA Security.
- Mid December 2009 – Operation Aurora, where hackers sought source code from Google, Adobe Systems and dozens of other high profile companies. .
- June 2009 – Stuxnet, spread worm which appears to have been part of a coordinated effort to reprogram a specific industrial control system, such as a gas pipeline or power plant, likely located in Iran.
- 29 March 2009 – GhostNet, cyber espionage which infiltrated at least 1295 computers in 103 countries, including those belonging to embassies, South Asian governments and the Dalai Lama. And many other attacks.

In the following lines we deliver the anatomy of APT and closing by the possibility and improvement of resilience to APT in organizations.

4.6.1 Anatomy of APT

The distinct attacking phases of APT are shown in simplified form in Figure 4.2 [47]. Where we annotated them as follows [34].

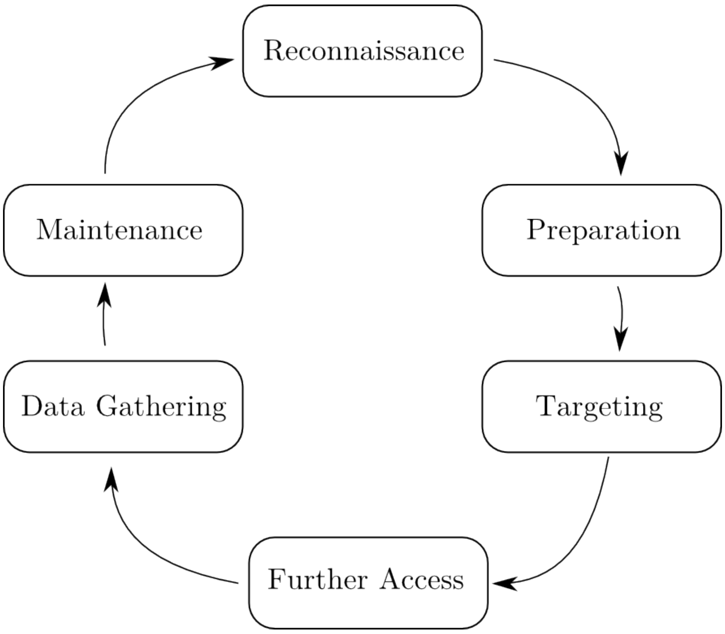


Figure 4.2: Basic APT attacking methodology

Reconnaissance

Is when the attacker passively gathers information about their target to identify the best targeting method. This may include research into the location of the target's offices, the location of their computers, technologies used by the company, how they communicate (between offices, with customers, suppliers and shareholders), their employees, their employees' contact details, interests and contacts.

Preparation

After the reconnaissance, the attacker actively prepares for the attack, developing and testing appropriate tools and techniques to target their intended victim. This may include scanning to determine vulnerabilities, writing malicious code or acquiring code, drafting socially engineered emails, determining which email account to send socially engineered emails from, acquiring necessary hardware (such as USB flash drives), determining what infrastructure to use to launch the attack and for command and control communications, registering for and setting up necessary accounts (email addresses, callback domains etc.) and conducting testing.

Targeting

In this phase the attacker launches their attack and monitors for signs of compromise or failure. The sender may attempt to connect remotely to a server to exploit a vulnerability, strategically place a USB flash drive or give one to a target, send socially engineered emails and if possible, check for bounce back notifications, monitor command and control infrastructure for beaconing activity from the victim, try to connect inbound to the potentially compromised computer, or await feedback from an insider.

Further Access

Once an attacker has successfully gained access to a computer network they will usually try to identify where they are in the network and move laterally within the network to access data of interest and to install additional backdoors. This will usually require a return to the preparation and previous targeting step, the upload of tools and malicious software, privilege escalation, network enumeration and identification of vulnerable hosts on which to install backdoors. It may also involve gaining access to the domain controller to obtain password hashes, covering tracks by altering logs, and accessing mail or file servers to enable data gathering.

Data Gathering

Once the attacker has identified information of interest they will try to gather this information and ex-filtrate it. They may do this using a *smash and grab* approach, trying to ex-filtrate the desired data before it is detected, or they may opt for a *low and slow* approach in which they ex-filtrate the data in small quantities over a longer period.

Maintenance

And finally, once the attacker has gained access to a network for information gathering purposes they will usually attempt to maintain their access. This may involve minimizing the amount of malicious activity they generate on the network to avoid detection, periodically communicating with backdoors on the network to ensure they are working as intended, and making changes as appropriate. If automated data gathering tools are in use, maintenance may also involve modifying search terms or the ex-filtration path, the volume or frequency. Maintenance also requires maintaining callback domains and any intermediary infrastructure used to communicate with the backdoors. If access is lost, the attacker may return to the initial reconnaissance or second preparation step in an attempt to regain access.

4.6.2 APT Countermeasures

To be able to improve resilience to APTs organizations should employ good security practices and policies including the following [34]:

- Information Centric Security Adopt. An information centric approach to security by applying multiple layers of security, affording the most sensitive information the most protection. If possible store sensitive information off-line, or on separate restricted access networks.
- Regular Patching. By patching operating systems and applications including document viewers (e.g. Microsoft Office, Adobe Acrobat) and web browser plugins.
- Computer Administration Restrictions. Minimize administrative access and restrict access so users do not possess both write and execute privileges for the same folder.
- User Education. Educate users on the threat from socially engineered emails and other forms of social engineering. Encourage users to notify IT staff of suspicious events.
- Network Access Restrictions. Restriction which computers can be placed on the corporate network via wired, wireless, and remote access methods.
- Known Network Topology. Ensure system administrators are aware of the location of all computers, computer equipment and Internet gateways so they can secure the network (including wireless access points and 3G USB modems).
- USB Drive Control. Restriction on USB drives can be used on corporate networks and develop policies on permitted usage and minimum encryption requirements.
- Intrusion Analysis. Conduct intrusion analysis (both host based and network based) to detect anomalous activity.

- Access Control. Employ two fold factors authentication where possible, particularly on Virtual Private Networks. Restrict user access using least privilege methodology, encourage good password control, regularly audit access logs, and review access levels.
- Sender Policy Framework. Employ the Sender Policy Framework (SPF) to help protect against spoofed emails. Where, the SPF is an open standard specifying a technical method to prevent sender address forgery [37].

4.7 Further Improvement

There are several potential values of further improvement of the current curriculum, however, we would like to develop this course not only to deliver and annotated the attacking phases and methods of attacks. Rather we would like to create a course with an wide range of content that will help in different needs. For instance, for developers, risk analysis, additionally by emphasizing the novel and favourable cloud security, security incident management, mobile application and penetration. Therefore, the under mentioned ideas are several subsets of potential future developments awareness, with a short description:

- Security Principles. To be able to develop secure software requires a great deal more than a mere knowledge of programming. The ability of understanding threats and risks in general, as well cryptography or security protocols is paramount. This section could discuss the issues relating to software and systems security, including banking and security evaluation.
- Secure and Robust Programming. During the programming level many system failures and security vulnerabilities arise. These can be usually attributed to inadequate handling of exceptional situations, such as poor understanding of the details of the programming language in use, incomplete descriptions of the interface, and insufficient care in the treatment of concurrency and threading issues.
- Trusted Computing Infrastructure. Widespread understanding of system architects is commonly deployed approaches to security however these have proven to be unable to deliver adequate levels of protection against today's threats. The technologies of trusted infrastructures are designed to address the problems by introducing new security primitives, based upon the inherent security of hardware solutions and the security issues that can arise in regard to the operating systems and their planned future development.
- Cloud Security. It is widespread nowadays and it is a new concept using old technologies. It is meant especially for commercial requirements and needs, and it has moved recently to academia. This section could cover the cloud computing architecture, management services and security challenges. Espe-

cially, presently when the lack of security results a high level of risks associated with cloud computing.

- Security Design. To meet security goals is increasingly important skill. This section could explore how cost-effective solutions of security needs can be achieved by following well established architecture practices and detailed security principles and to strike the balance between security and other system requirements.
- Risk Analysis and Management. Risk is an essential component to computer and information security, as is understanding the exposure of the system to different threats enables security efforts to be prioritized. Through measurements and estimation of risk, security can be managed and cost benefit decisions can be made. The principles and tools behind risk analysis for security could be explored and thus practical experience on a realistic case study could be provided.
- Forensics. Legal evidence found in computers and digital storage media, by examination, identification, preserving, recovering, analysing and presenting facts about the founded information. We could note the forensic principles and techniques related to the investigation of software and systems, and how the results of an investigation relate to the security measure that were taken during the development and implementation of a software.
- Data Security. Increasing amounts of data are captured, linked and utilized for many different purposes. Therefore, the awareness of both the risks and threats associated with data security as well as the relevant legislative and regulatory frameworks must be implemented.
- Security and Incident Management. To deliver the key themes and principles of security incident management, and to be able to implement these principles in designing systems and models for managing security incidents.
- Mobile Application Security. Mobile malicious codes are rising and the development should involve a good practice of security design. In this section we should demonstrate how to identify and analyse malicious code in the mobile application.
- Penetration testing, in other words pentest. It is a method of evaluating the security of targeted system or network by simulating an attack with in malicious code. This could be very handy and useful for organizations before they release their product, services or application, to test the security level and to perform hence action for securing. By delivering different methods and standards of pentesting, and in addition for the web application penetration testing.
- Malware analysis. To deliver the different types of malware and advance defensive techniques, followed by providing the latest trends in honeynet technology. In addition, how to catch malware, through virtual environment machine and

guest set-up or using Dionaea[17] software, and alternatively, initial analysis of malware, such as static and live analysis and Norman Sandbox[18] technology.

The above list is just an undermined list for a future development of the advanced curriculum course. And in the end, it will be extremely interesting and favourable for any type of organization.

[17] Dionaea: `http://dionaea.carnivore.it/`, last checked 21.04.2012

[18] Norman Sandbox: `http://www.norman.com/security_center/security_tools/`, last checked 21.04.2012

5 Management

Information security management is a structured process for the implementation and ongoing management of information security in an organization [62]. It includes activities that aim protecting information and information facilities so as to secure business continuity. It is therefore important that information security management is treated like any vital business function, with all its activities based upon business needs [4].

Nevertheless, obviously all managers are users, but on the other hand all users are not managers. In the third and final course of this awareness program we will focus and disclose the issues that could arise in the organization intended for the management staff. In fact, we would like to stress the importance of understanding the decision making process especially nowadays that the management staff in any organization deals with and has to find answers to every day incidents that arise because of of information security.

However, in this chapter we discuss the phases of decision making process, in detail by PDCA and OODA cycle and closing by the further improvement of the curriculum where we include cost optimization and cyber security awareness.

5.1 Decision Process Making Phases

Literary organizations operate by people making decisions. For instance, a manager plans, organizes employees, leads, supervising, and controls the team by executing decisions. Different teams, requires different approaches, for example the development team needs a development approach of securing their staff, client information and the application information, which is different to what the human resource team requires, where they have to implement a disclosure of securing the customer and clients information and so forth. However, the effectiveness and quality of those decisions determine how successful managerial staff is.

Managers are constantly called upon to make decisions in order to solve different level of issues. Decision making and issue solving are ongoing processes of evaluating situations or problems, making choices, and following them with the necessary actions. Although sometimes the decision making process is very short, and mental reflection is essentially instantaneous. While in other situations, the process can be carried on for weeks or even months. The entire decision making process is dependent upon the right information collected, being available to the right people at the right time.

For instance, the decision making process sometimes can involve the following steps:

1. Define the issue.
2. Identify limiting factors.
3. Develop potential alternatives.
4. Analyse the alternatives.
5. Select the best alternative.
6. Implement the decision.
7. Establish a control and evaluation system.

Moreover, in terms of information security, a management system allows an organization to [13, p. 14]:

1. Satisfy the security requirements of customers and other stakeholders.
2. Improve an organization's plans and activities.
3. Meet the organization's information security objectives.
4. Comply with regulations, legislation and industry mandates.
5. Manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals and to the environment.

However, the organization should have a process approach to identify and manage many activities in order to function effectively and efficiently. Most of the activity using resources needs to be managed to enable the transformation of inputs into outputs using a set of processes, or in other words interrelated or interacting activities. For instance, the output from one process can directly form the input to another process and this transformation is carried out under planned and controlled conditions. It is therefore, this system of processing within an organization, together with the identification and interactions of processes and their management, can be referred to as a process approach.

In the following section the process approach we will disclose the two types of four-part cycle. However, we annotated to the participants that there is a difference between the PDCA and OODA loops, during the explicit inclusion of sense-making, or in other words orientation. In addition, according to David Lancey[1] he PDCA loop is slow, where he emphasizes that it is typically translated to an annual budget-driven cycle in contrast to the OODA loop which is all about the speed.

[1] David Lancey Blog: `http://www.computerweekly.com/blogs/david_lacey/2012/02/the_wrong_type_of_loop.html`, last checked 17.04.2012

5.1.1 Plan–Do–Check–Act

PDCA was developed by Dr. Walter Shewhart a father of modern quality control. The process approach is based on the operating principle adopted in ISO's management system standards, and commonly known as the PDCA - Plan - Do - Check - Act process [13, p. 14], see Figure 5.1.

- **Plan**. Establish objectives and make plans by analysing the organization's situation, establish overall objectives and set targets, and develop a plan to achieve them, identify the potential risks, articulate the legal requirements, and establish the responsibilities, resources, control, risk acceptance criteria, and procedures needed to prevent breaches and manage them when they do occur. In detail, this phase implies planning and building a concrete plan for future actions. In other words, it is an essential start up of every decision making process, without a plan or objectives we will not be able to follow any further actions. The importance of establishing and developing a concrete analysis of the issue is evident. Moreover, developing a process will help and lead to the implementation of this plan. However, this plan sometimes could take a long period of time to be finished, or to be entirely developed. This phase is considered to be made up of two parts. The first, is to determine the goals and targets. And secondly is to determine the methods of reaching those goals.
- **Do.** Implement plans and do what was planned to do. After the plan has been accepted and developed, the next approach is the implementation of the plan. Moreover, this phase enables for instance the security management team to implement their plan and manage the day-to-day security operations. Sometimes, in this phase it is necessary to go back to the first phase, if during the implementation there is an issue, and the best way of bypassing the breach and speeding the decision making process by returning to planning and this will help to pervade. This phase also includes the engaging of education and training, and the process of how to implement the work.
- **Check**. Measure results and monitor the extent to which achievements meet planned objectives. In addition, it includes activities such as detecting an attempted or successful breach, to determine how the breach occurred and how it was handled, reviews and measures the effectiveness of the controls in place taking into account any changes to the company's organizational structure, people, processes, or technology, and finally update their plan. After taking a decision, always check before acting. In more detail, this phases refers to measuring and monitoring the results to control that the objectives of planned situation are fulfilled. One of the best ways of achieving this, especially in technologies, is to use the large amount of tools and applications that could aid in monitoring and measuring and testing the objectives. Finally, check the effectiveness of implementation.

- **Act**. The final set of processes concentrates and stresses on correcting and improving activities by learning from mistakes so as to achieve better and extremely valuable results. It is in this phase that the security management team can apply the lessons it has learned from this experience and implement the necessary improvements, and communicate their actions and improvements to the interested stakeholders to ensure it satisfies their requirements. In other words, taking an appropriate action. Usually, after this phase has been complied with it goes all over again from the beginning and other or additional objectives are established to meet further plans.

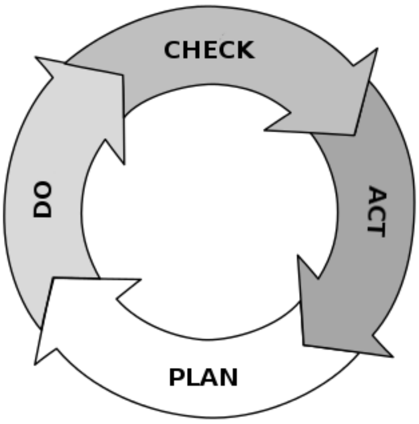


Figure 5.1: The PDCA loop

Obviously, this is just a very simplified account of how the PDCA processes might work for any requirements and expectation. Although it is slow to implement, yet indeed it adds improvement and effectiveness into decision making processes. Closing, it is a reverse loop and could go all over again until it reaches the objectives and the requirements.

5.1.2 Observe, Orient, Decide, and Act

Most of the actors in our case, the managers are attempting to achieve decision superiority by making better decisions more quickly. On the other hand, adversaries attempt to prevent decision superiority by conducting offensive information operations that with the intent to corrupt their opponent's decision-making processes [43]. This leads to the actors not being able to enact good decisions because their remarks are corrupted and hence they cannot be converted into satisfactory intelligence. There are plenty of ways to disrupt the OODA loops feedback cycle, for instance, through physical attacks and psychological operations. In this paper we focus on the cyber activities that could occur.

We have already mentioned the two specific OODA loops: BMD OODA loop and Cyber OODA Loop. In this paper we concentrate on the Cyber OODA loop.

The Cyber OODA loop is the decision-making process that enables cyber attack defence, Figure 5.2 graphically graphically presents a simplified graphical view of the OODA loop [38, p. 3]. It facilitates the observation and analysis of cyberspace and enables decision makers to enact defensive countermeasures [38, p. 3].

- **Observe**. It is an initiation and instinct phase of the decision making process. Observation refers to the necessity of becoming aware and knowledgeable, especially through careful and directed attention. It is necessary to observe what is happening and to determine the circumstances under which the decision must function. Additionally, it is a phase where the data of situation analysis is collected. Next, is the orientation phase involves the analysis process in which data is interpreted into usable information.

- **Orient**. After the data on the situation is collected, it must be mentally synthesized into information. In other words this phase is also known as recognition. Orientation and recognition is about making sense out of the observations. It is where an initial assessment begins and a mental picture is created. Primarily, new data is introduced from the observations of the environment and the situation and then it is merged into the existing framework and a process of destruction and creation occurs. When it is incorporated, the current image is destroyed and a new one which embodies the new data results from the merging of the observations, the situation and the former framework.. The destruction or creation process varies from person to person because it incorporates unique personal characteristics such as experience and culture. However, the image which is formed during the orientation serves as the foundation upon which the decision will occur. This phase also interacts with the observation and the decision phases because changes in the image leads to additional data collection forays and can also change the way decisions are made, in other words decide. The speed of these phases is extremely important. The observation and orientation/recognition phases are included in the part of the decision process where data is gathered, synthesized and interpreted. After orientation is accomplished, a decision can be made.

- **Decide**. Is the third step in the OODA loop. The decision-maker evaluates the information acquired during the first half of the cycle. It is in this phase that the decision-maker considers possible options and chooses which ones to pursue. The amount of information data necessary to come to a decision varies. However, every decision requires a minimum amount of information before it can be reached. Since the minimum level of information has been obtained to information and data gathering, opportunity is lost and a problem situation evolves. If the problem is put aside, the problem will grow to crisis proportion. Therefore, decisions need to be made and then acted upon as soon as the minimum information and data is acquired.

- **Act**. The final phase of the cycle is action. Previous efforts, which culminated in a decision, are put into effect. If the observation of the actions results occur, and the cycle is repeated again and again.

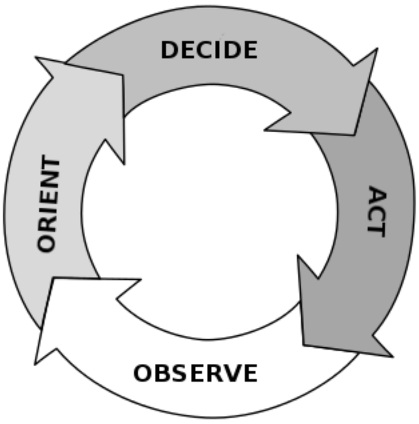


Figure 5.2: The OODA loop

The length of time needed to go from observation, the first phase, to action, the last phase, is captured in the OODA loops diameter. Using a shorter amount of time to move from observation through to action is depicted as a smaller cycle, while a longer time is shown as a larger cycle [50, p. 46].

5.2 Further Improvement

Future development idea of management course curriculum could include the following segments:

- Risk management is wide area when it comes to information risk management or cyber security risk management. The key methods that could be introduced to the participants, could be such as: the efficient use of resources, internal controls, information sharing, technical improvements, behavioural/organizational improvements, and cyber security insurance. On the other hand, in risk management, we could include risk avoidance and mitigation within the foundations and management of cyber security.
- Information and cyber security assurance in organizations, that is, what has to be done to implement the best security measures in organizational level in main security activities area, like implementing the dependency matrix of Graded Security Model (GSM) [31], and additionally the security goals can be specified, such as: organization of information security, human resource security, physical and environment security, access control, information security incident management, asset and business continuity management, and many others.

- Another extremely important factor that managers have to deal with is security management and cost optimization, which is influenced by human, content, time and performance management.
- Security standards and implementation such as, COBIT [1], PCI data security standard (DSS) [44], ISO/IEC for example ISO 27002:2005 [29] and many others.
- Another, importance is how to manage and create working flow policy and privacy for organizational needs, and how to implement and improve the technology, Implementing Information Security Management System (ISMS) will demonstrate a proactive approach to continuously and effectively manage, at a high level, information security by including people, infrastructure and businesses. The goal is to reduce risks to manageable levels, while taking into perspective both business goals and customer expectations [45].

This is just a small amount of extremely valuable and favourable segments that should be implemented and improved in the management curriculum.

6 Course Management System

We have developed a prototype web based application for the management of the syllabus available to a worldwide audience. The application provides two user friendly interfaces: students and administrative interface. Although most of the content and course material are available without any requirements of registration, still a non registered user will not be able to view the questions of the units, scoreboard and topic adviser. Therefore, if the user wants to take a part of measuring his knowledge we provide a simple, automatic and free registration form which requires a valid e-mail address to confirm the activation code.

In addition, the application provides a discussion board. There are three types of discussion boards: suggestions, ideas and questions. Topics in the suggestion board are more likely to be taken into consideration and implemented, while the idea discussion board is for topics that the user does not really want to be implemented and each participant can hold conversation in the form of posted messages, in the question board where he can discuss questions and interact with other students. Students are not allowed to post solutions to questions, but they are allowed to discuss the material covered in class; and of course pose questions. Similarly, we provide a Frequently Asked Question list (FAQs), to alleviate the workload of veteran readers from answering the same question over and over as new users enter the course. They are list of hyper-links as question sentences, which associate the answers to the questions.

Alternatively to student interface, the administration interface offers possibilities of creating new courses, modules, units, quiz's and records of right answers. Additionally, the administration will be able to edit the results from the baseline service.

Furthermore, Course Management System (CMS) or in other words learning management system (LMS) is a software application for administration, documentation, tracking records, scoreboard and reporting of training program and training content. Our prototype system is developed in CodeIgniter[1], PHP[2] framework in addition MySQL[3] relation database management system. The current version of the application is added to the CD of the prototypes. However, this application requires further development.

In the following chapter we will discuss the usability of the user interface and profile. This is then followed by the user scoreboard and the topic advisor. We also include

[1] CodeIgniter: `http://codeigniter.com/`, last checked 17.04.2012

[2] PHP: `http://www.php.net/`, last checked 17.04.2012

[3] MySQL: `http://mysql.com/`, last checked 17.04.2012

usability and possibilities into the back-office or in other words administration user interface. Finally we present what should be considered and taken into account for further improvements and development. We conclude with the content of the prototype on the CD.

6.1 User Interface and Profile

The goal of the user interface is interaction between users, humans and the machine. Thereby we have developed an interactive user interface, where the users, participants of the syllabus can effectively participate into the awareness program course. As mentioned previously the course is available to everyone at no charge and no registration fee. However, if the participant desires to understand progress in the course he is required to register for free with a valid e-mail address to be able to receive the automated random generated activation code, in other words, the link. After the registration process is completed the user will be redirected to provide and answer the baseline survey, for more info about the survey template please refer to Appendix section. The survey is provided through open source solution Kwik Survey[4].

Furthermore, the course interface is illustrated in Figure 6.1, where letter A is a sidebar, list of courses, modules followed by the units, moreover letter B is illustrated box of video for the unit, after ending the video automatically presents the questionnaire quiz for the unit. Additionally, letter C delivers a description of the unit followed by the hints link, in other words links or an indirect suggestion for more beneficial answers to the questions. In the example the participant is in *Basic* course, module *Physical Security*, followed by *Protect Your Computer*.

In the field B, videos are merged from beforehand uploaded videos on YouTube[5] video sharing website. We have chosen Youtube because of the caption and subtitles feature, which gives viewers a deeper understanding of the video, either because they speak a different language, or because they are hearing impaired. These features can assist in translating the lectures, videos into different languages for future improvement. After the user has completed the questionnaire quiz and provided the necessary answers to the question they are automatically redirected to the next following unit and if there are no more units for the current module they will be redirected into the next module.

In addition, there are two types of questions: single choice and multiple choice questions. Firstly, single choice questions provide the participants with a list of possible answers, where only one answer of the possible choices is the correct answer. Secondly, multiple choice questions are a form of assessment in which respondents are asked to select the best possible answer or answers of list. For single choice

[4] Kwik Surveys: `http://kwiksurveys.com/`, last checked 17.04.2012

[5] YouTube: `http://www.youtube.com/`, last checked 17.04.2012

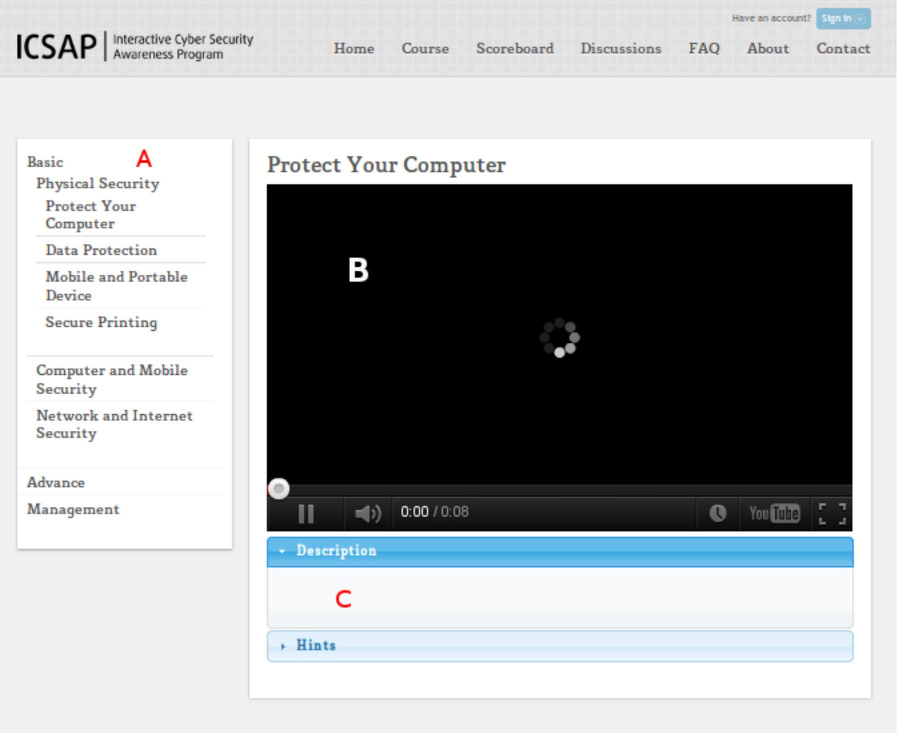


Figure 6.1: Illustration of User interface (A - Sidebar - list of course, modules and units, B - Box for videos and questions, C - Details of course, module, units and hints)

question if the respondent answers correctly he scores one point, otherwise no score is earned score for this. In contrast to single choice question, scores in multiple choice questions are earned for each correct answer given, where each answer equals one score. All in all, scoreboard details are highlighted in the following subsection. It displays scores earned for each single unit, module and so forth. We have also grouped questions and units into different topic advisors, handy for advising the participants on their weakness areas and hence profitable action can be taken.

Although the user interface and profile functions, still further development and improvement of the system should be considered. However, usability is valuable in the system, whereby the user can change user data, for instance password, e-mail, etc. And can extend communication with other participants to share ideas, suggestions and questions.

In the following subsections we will highlight the principles of scoreboard and the serviceability of topic advisor.

6.1.1 Scoreboard

The scoreboard functionality is to expose the number of points gained throughout the quizzes spread during the videos. Each quiz consists of one or more questions. It will show how many questions the participant answered correctly out of the total number of questions for each unit (correct/total). The percent correct is computed by summing over the number of correct answers and dividing by the sum of total questions. So for example, if the participant completed a unit with four questions and had the following scores for each quiz (first number of question pair, second number of each pair of earned score) 1/0, 2/1, 3/1, 4/1, the final score for the unit of the module would be (0+1+1+1)/4 = 75%. At the end, after completing the entire course, the total score is computed by summing the number of correct answers of all units and dividing it by the sum of total unit's questions. For instance, if the participant answered 61 questions correct, out of a total number of a 70 question course, the final result of the course is 61/70 = 87%. The statement of accomplishment will be sent via e-mail and signed.

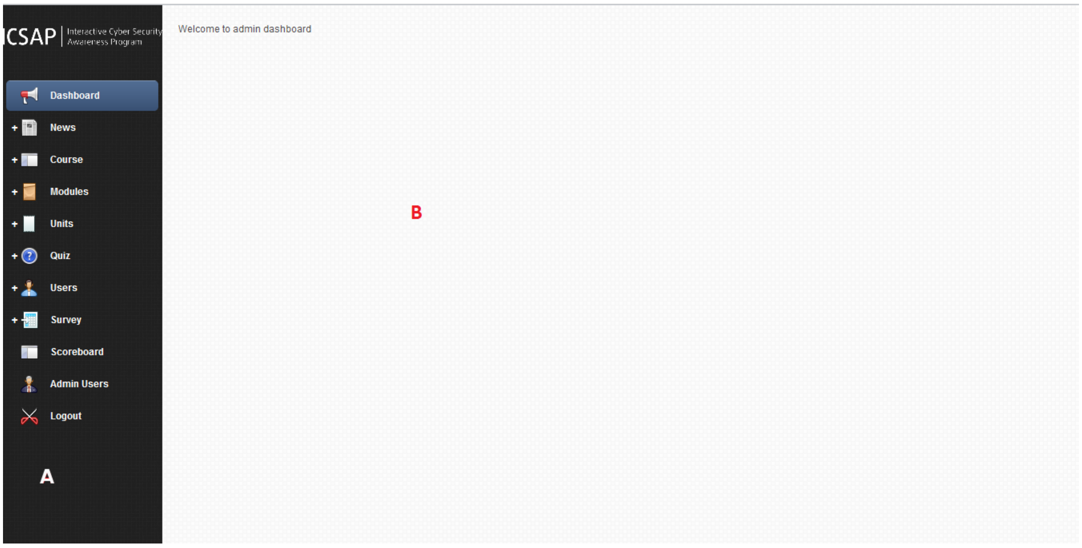
The novel approach of this syllabus is that it can be interpolated into the demands of organizations or businesses where it can provide extremely productive and undeniable security awareness. Thus the formation can distribute an accomplishment and benefit for the participants and employees.

6.1.2 Topic Advisor

The superior idea of topic adviser is to lead the participants for a future action if needed. The questionnaire quiz questions are divided into different groups. In other words, some of the questions are for personal use and others are more for organizational/corporation level use, therefore the courses deliver diverse topics. However, if the participant for instance answers incorrectly to a type of question which is linked with personal information or personal usage, the adviser will count the points and if the point is less than an emphatic level, we will address on the scoreboard that future action should be taken in consideration. Otherwise will not display the weakness, where future action is not need it. The purpose of this topic adviser is extremely profitable for participant and the organizations benefits. Further improvement and development should be considered.

6.2 Administration

The goal of the administration interface is to help the administration of the course to document, track and continue managing the course. For instance, to upload new content, new course, module, units and so forth. Additionally, the administrator can add news, track the record of the baseline survey, questions, answers of the users, etc. In Figure 6.2 we have illustrated the administration user interface, where letter A is the sidebar where the administrator can view and edit the content of subject matter into the letter B, the main content.



Welcome to admin dashboard

Figure 6.2: Illustration of Administration user interface (A - Sidebar, B - Main content)

The following tasks can be accomplished by the administrator user:

- Can edit, view and create news, which are exposed into user interface on the first index.
- Can edit, view and create new course, for instance: basic, advance and management course.
- Can edit, view and create modules for a specific course.
- Can edit, view and create units for modules which are linked to a course.
- Can edit, view and create new questions, followed by providing two possible ways of providing answers: single choice and multiple choice answers. Additionally supply the correct answer.
- Can view and delete users data and profile information.
- Baseline survey is through Kwik Survey[6] open source application for designing surveys, forms, polls and feedback form and the results of the responses can be seen.
- Scoreboard can be only viewable and filtered by needed operations.
- Admin users allows the administrator to add, view and edit administration users details.

[6] Kwik Surveys: `http://kwiksurveys.com/`, last checked 30.05.2012

In fact the administrative interface is still in development prototype version rather than to be used for production, however it requires further improvement.

6.3 Further Improvements

Although the user and administration interfaces are user friendly, we would like to emphasize the importance of interaction between humans and machine through testing, development and improvement of the interface. Another superior approach is by implementing the valuable baseline survey into the system, rather than using the third party solution. In addition we have also applied the improvement of attractive scenarios, video interaction, questionnaire quizzes, and effective delivering of results. As well as intriguingly to enforce the program into public organizations, where convincing action should be taken to raise the awareness level of cyber security.

Nevertheless, we have highlighted below the improvements that are the first priority of important action.

- Course Management System
    - Baseline survey: implementation of own survey solution, rather than using the third party open source, for user and administration.
    - Discussion board: change the Google moderator[7] solution with own, or with additional installed open source forums or discussion board solutions.
    - Better viewable scoreboard, where we could provide more details and mistakes made by the participants.
    - Export of data into different format files for better and quicker proceedings and analysis of data, for instance: excel format, or CVS file format.
    - To be able to provide an open question quiz, where the participant could write down the answers.
    - Translation of the entire content into different language, as well the videos. This should serve the hearing impaired and break down language barriers.
    - Clear and more adept terminology.

6.4 Prototype on the CD

This thesis is accompanied by a CD which contains the prototype of the web application, including the MySQL script. The short description of the contents of this CD can be found from the README file.

[7] Google Modelator: `http://www.google.com/moderator/`, last checked 30.05.2012

7 Results

The study will begin by outlining the main requirements that have been taken into account when supplying the participants with the online awareness training courses. Where evaluation and feedback mechanisms are critical components of any security awareness program. Therefore, the study address a computation of baseline survey, where the questions are presented in Appendix section and comparison of results of questionnaire quiz completed by the participants. Then in the end, we have presented the feedbacks, suggestions and the ideas from participants.

Presently this study provides entrance for participants only with Basic curriculum and the relevant questionnaire quiz. Where the intention of baseline survey is to determine, how the participants access the Internet; where they use computers; what they consider as the greatest threats in information technology and how they are concerned about the safety of their information technologies assets; what measures they have taken into account to protect their computer and electronic data; and in the end, what is the best way of providing information about how to protect the participants from the potential dangers of information technologies. On the other hand, the purpose of the questionnaire quiz after each unit is to display the raised knowledge gained during the learning process of the curriculum.

The following section sets out to examine the prior and consequently the raised knowledge gained through the research problem in detail.

7.1 Baseline vs Awareness level

The focus of the study is to examine primarily the response to the prior concern about the safety and knowledge for protection of information assets compared to the scores earned or gained in the curriculum.

In general a large percentage of participants are accessing the internet through different types of broadband communication technology used for connecting to the Internet. Where the usage of computer is typified. Moreover, the concern about the safety of their information technology assets, such as, the computer and laptop, peripherals, electronic data and mobile devices are aligned and it ranges from extremely concerned to least concerned. Likewise, the range in a scale of extremely knowledgeable to least knowledgeable about protecting their information technology assets is very diverse. Furthermore, the greatest threats to their information technology are by a systematical approach to the most commonly known threats. Thus, the in placed protection used for their computer and electronic data is coherent. However, the best way of providing information on how to protect themselves from potential dangers is considered through online training.

Figure 7.1 shows in detail one of the obvious methods of accessing the Internet is through different types of broadband communications technologies, exactly 87%, where there is a significant difference between companies, schools internet and mobile broadband access. On the other hand, Figure 7.2 represents the places where the participants use the computers. The participants use the computers either from home, office, school, library, bus, train or on the move by using laptop, notebooks, tablets and mobile phones. We can note that only a very small percentage of participants use the computer in an Internet café.

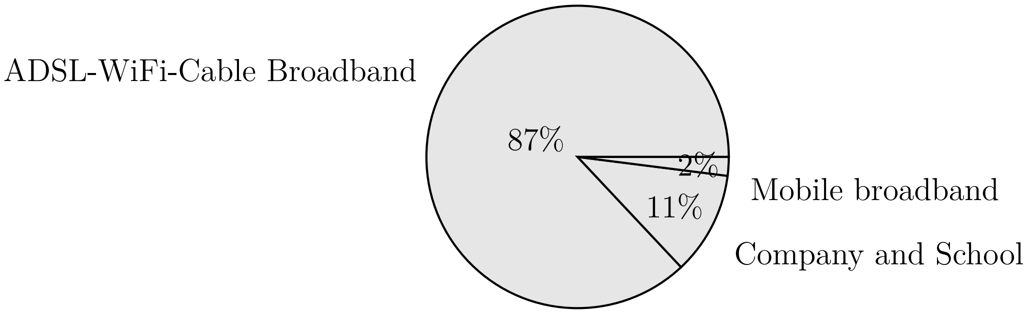


Figure 7.1: Accessing the Internet

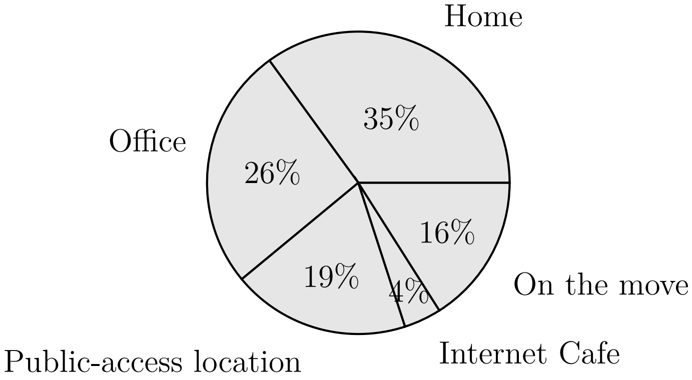


Figure 7.2: Usage of computer

Meanwhile, from the graph Figure 7.3 we can note that many of the participants nowadays consider that the safety of their computer is essential. Instead, only 33% of the participants slightly consider protection of peripherals and electronic data as necessary. It is also interesting to note that a greater number of the participants are least concerned about protecting their mobile devices. The participants considered safety as protection from adverse effects, on a scale of one to five; with one being very concerned, and five being the least concerned. Thereby the support for this interpretation comes from Figure 7.4, where a large percentage of the participants consider themselves somewhat knowledgeable in protecting their information technology assets. There is a marked similarity between the very knowledgeable and least of knowledgeable.

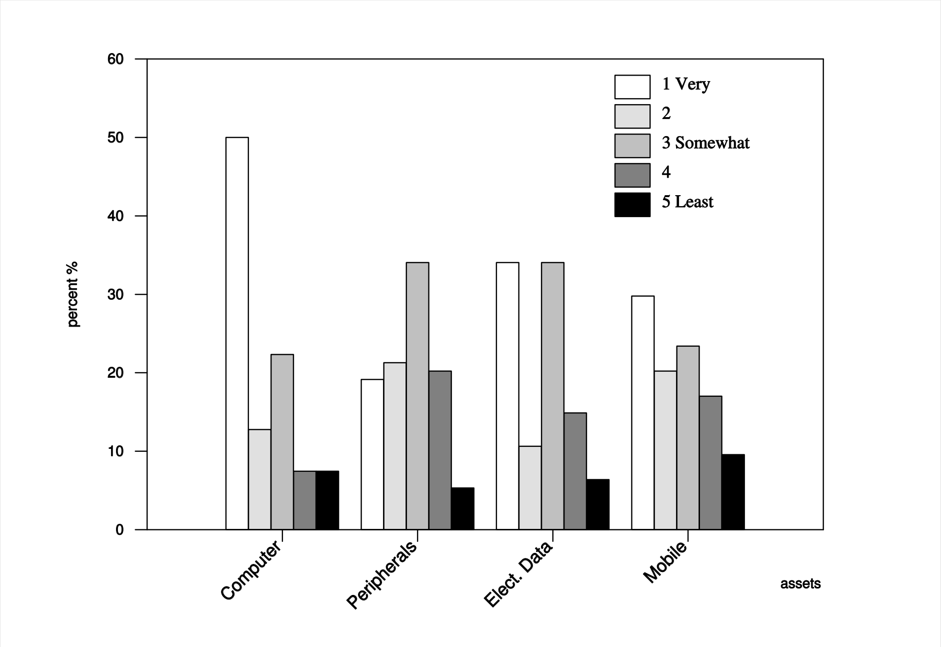


Figure 7.3: Concerned scale for IT Assets (1 - very, 2, 3 - somewhat, 4, 5 - least)

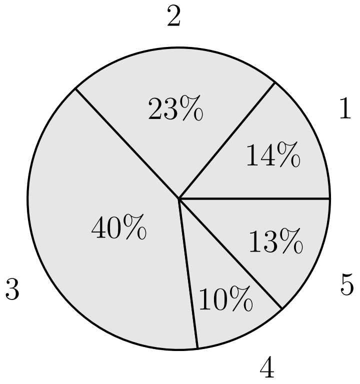


Figure 7.4: Knowledgeable protection of IT assets (1 - very, 2, 3 - somewhat, 4, 5 - least)

However, the greatest threats to their IT assets can be clearly divided into three groups. Figure 7.5 illustrates that the participants consider viruses, worms, hackers and intruders as the highest threats. Instead by malicious software (e.g. spyware), spam and other unsolicited emails are considered much less significant. The least significant threats are considered by the participants to be the fraudulent schemes and faulty computer hardware. Additionally , the participants have indicated other factors of threats, such as, USB viruses, service providers and people not protecting their personal info.

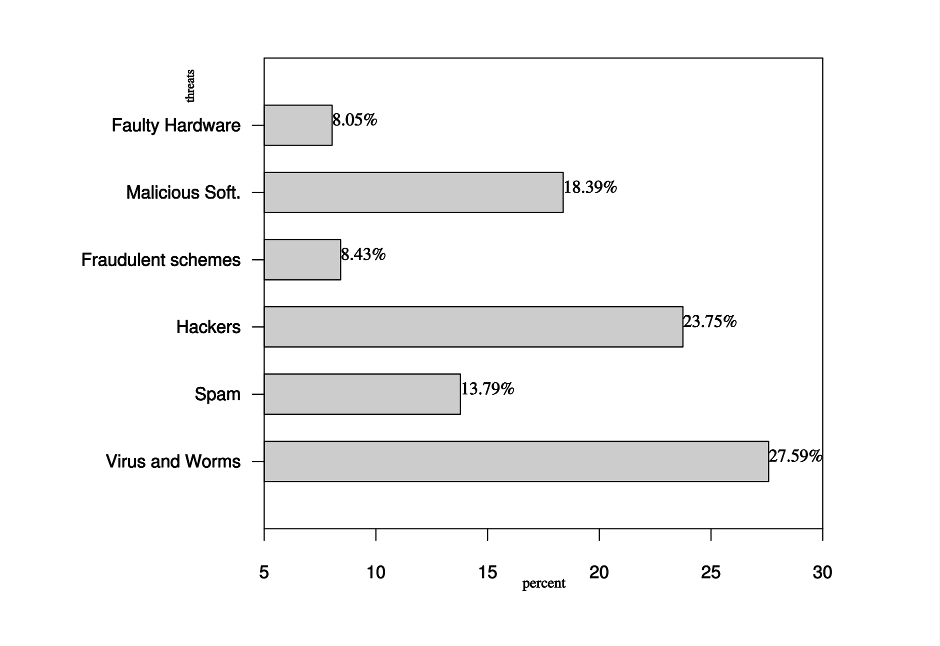


Figure 7.5: The greatest threats

Moreover, the survey questions ask what kind of protection is in place for protecting their personal computer or electronic data. The results are presented in Figure 7.6, where the highest ranking is antivirus software that is updated regularly, followed by the firewall. Next are good password practices and an up-to-date Internet browser with encryption. And finally, the lowest ranking are locked screen saver on their notebook/mobile phone/tablet PC, anti spam filter and process of regular backup of data. However, few of the participants indicate that the above list does not work, or they have none listed protection because they use Linux operating system, and one participant noted that he is using additional anti malware software.

The best instrument to provide the participants with information on how to protect themselves from potential threats of IT assets is drastically underlined through online training. Figure 7.7 clearly indicates that online training meets the needs of 43% of the participants as the most effective method, followed by online adverts. Then by radio or TV adverts, and the least possible way of distributing information about security is by newsletters and posters. Other options given by the participants as, potential ways of providing information on how to protect themselves included providing computer courses, IT magazines, online forums and security conferences, from friends, and by interactive presentation with short and clear info.

Nevertheless, the basic curriculum consists of three modules, where each module is divided into units. And each unit presents a questionnaire quiz - test where the

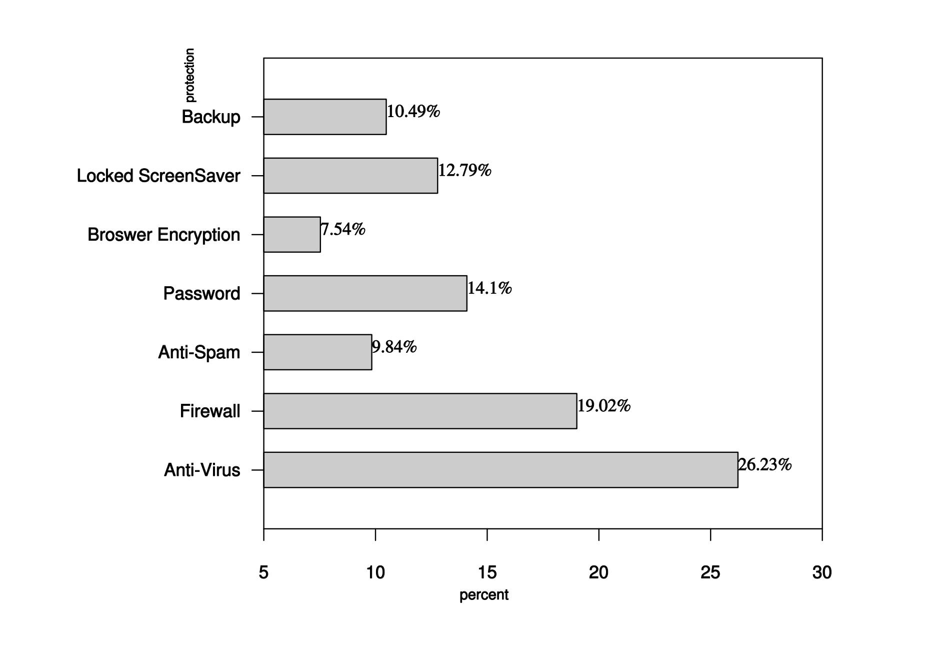


Figure 7.6: Protection solutions that are placed

participant can provide answers to the questions which have single or multi choice answers. There are a total of 54 questions in the basic curriculum and the age difference between participants starts from 11 to 63 years old, where 69% are males and the remaining 31% are females. The following lines set out the results from the Basic course of each module, computed with the average percentage score results for the units. In the end it presents the raised awareness knowledge achieved through the interactive online course.

The basic course is divided into three modules: physical security, computer and mobile security and finally, network and Internet security. Each module is divided into units, for instance, the physical security has four units: protect your computer, data protection, portable and mobile device and secure printing. For computer and mobile, and network and Internet security please refer to the third chapter, or Table 7.1. However, Table 7.1 is interesting in several ways. First it demonstrates the average percentage score gained from answering the test in each unit from the participants. Secondly it allows us to pinpoint units in which participants are more knowledgeable and in which units they are less knowledgeable so as to take tailored measures for future actions. Where, Figure 7.8 presents the average percent score achieved by users in modules. Such as, physical security, which indicates 60%, then for computer and mobile security the average score gained by the users in the inside units is 64%, and finally, for the network and Internet security module average score gained by the users is 70%, which is also the highest score.

Furthermore, Table 7.1 compares the average percent score gained for each unit in the three modules. For illustration, in the physical security module, mobile and

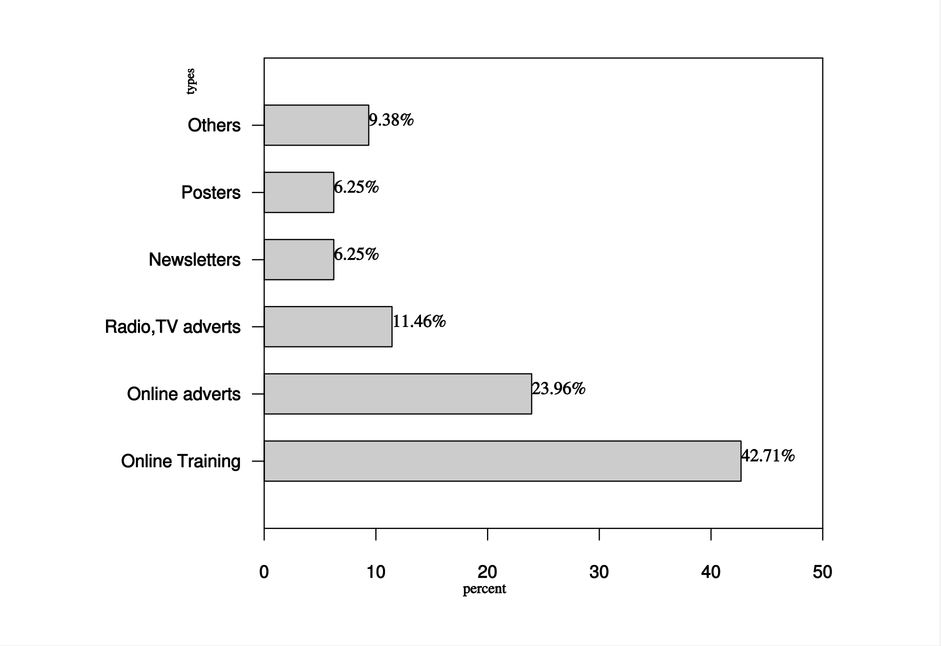


Figure 7.7: Types of providing information on how to protect

portable security unit had the highest score, especially the secure printing unit has the lowest score. Where, in computer and mobile security module, malicious software and strong and safe password units are practically at the same level with average score percent, different from operating system security. And in the last module, network and Internet security, the highest average percent in score is obtained in the secure browsing unit.

The present findings suggest several courses of action in order to solve and elevate awareness knowledge, by positive results. Results so far have been very encouraging and they have confirmed that the method and approach of our interactive cyber security awareness program are decisive and invincible. The implementation of the syllabus will improve everyday work and usage of computers, mobile phones, online banking, social networking, etc. As well as, needed future action.

7.2 Feedback, suggestion and ideas

We have received very valuable feedback, suggestions and ideas concerning the cyber security awareness program from the students participating in the basic course. One of the most important challenges for us is when the students have very different background and previous knowledge. For instance, people who knew more about secure browsing did not have so much experience with e-mail and instant messaging security and vice versa. Therefore, it is actually a good idea to cover a wide range of topics including network, physical, mobile and application level security issues.

Basic Course	
Physical Security	Avg. %
Protect Your Computer	52.86%
Data protection	65.09%
Mobile & Portable Security	67.24%
Secure Printing	48.67%
Computer & Mobile Security	
Malicious Software	67.50%
OS Security	61.96%
Strong & Safe Password	66.05%
Network & Internet Security	
Social Engineering & Social Networking	65.38%
Secure Browsing	85.71%
E-Mail and IM Security	57.14%
Firewall	67.14%
Wireless Networking Security	68.57%

Table 7.1: Basic course, modules and inside units, earned average percent score

Network and Internet security seemed to be the most well-known theme. Some of the students pointed out that they did not learn anything new from that module. Many others on the contrary, were not so confident in this area, and they have become aware of social engineering and commonly known security issues about wireless networking after completing the course. In future, we should prepare fewer but more advanced and useful tasks dealing with network and internet security.

In general, the participants found the topics and units interesting. Although many learners had quite good theoretical background about the threats of IT assets, they thought it was useful to practice the theory and best known practice. Even a person more competent in computer and mobile security than we are, said he was able to learn some new tricks and that the quizzes were exciting. Another detail pointed out was that whilst you may often read about new vulnerabilities or security problems, you usually just don't have enough motivation or time to delve into practical security. In conclusion, we find that the selection of topics is quite effective, although future improvement can be considered. Naturally, we need to keep the list of the themes up to date and seek new interesting ideas.

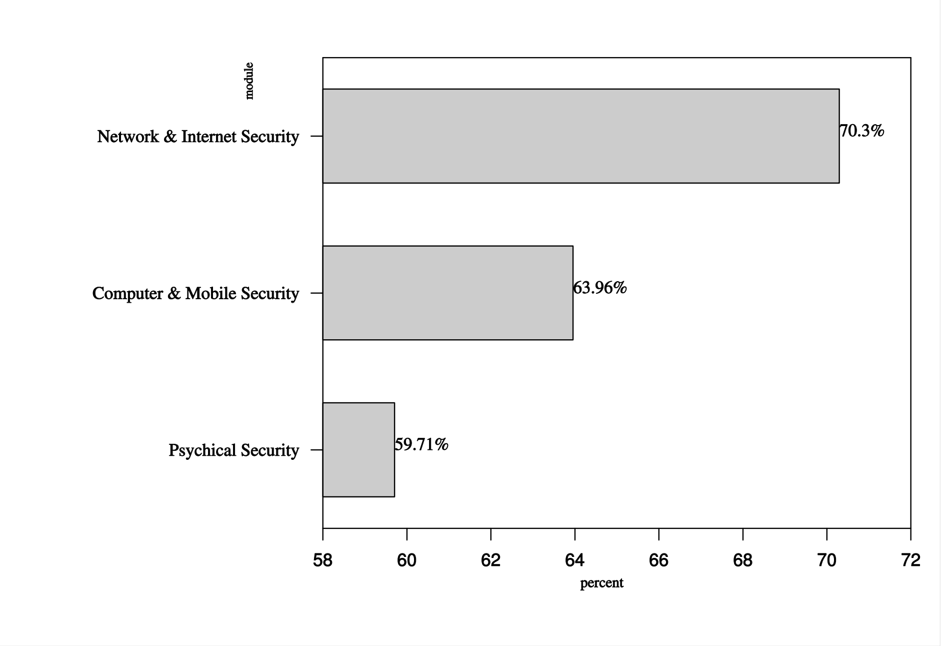


Figure 7.8: Average percent score gained by modules

8 Conclusion

The threats to cyber security are constantly evolving. Thus we need to ensure that not only the specialists who are protecting IT systems get a proper awareness education, but also the basic, everyday users and managers should too. In the first chapter of this thesis we reviewed a number of related works which discuss the issues associated with conducting practical awareness educations for information and valid cyber security courses. The general conclusion is evident, active learning methods are considered to be extremely beneficial, and diverse level groups are fundamentally conclusive.

We have prepared a set of educational tools and a practical syllabus to support information security awareness using the obedient approach and to help in the development of information that can raise awareness of the importance of information security. The syllabus is organized into a systematic approach of three important groups:

1. The introduction is “Basic”, which aims at delivering to everyone an elementary curriculum course for physical security, computer and mobile security and network and Internet security.
2. The “Advance” program primarily demonstrates the attacking phases, different attacking methods, followed by countermeasures that show the anatomy of Advance Persistence Threats (APT). And it is intended for administrators, help desk personnel, information technology professionals and so forth.
3. The last course “Management”, illustrates two decision making processes with their cycle loop.

Additionally, after each unit there is a questionnaire quiz, which measures the knowledge of each participant. This is then compared to the baseline survey undertaken during the registration process which helps us to determine the participant’s prior concern about the safety and knowledge of protection of information assets. The syllabus imparts knowledge to the participants on how to be aware of information technology protection approaches and threats. In addition, in this way the participants learn the methods and tools on how to protect themselves, and how to use the methods of the attackers, which in the turn helps the user to choose better defensive strategies, technologies and solutions. We are not aware so far of any syllabus that has previously used this method and approach. We believe that our unique contribution is important and valuable to information security and cyber security education, because we have introduced ideas, systematical methods and solutions that have been proven to be successful elsewhere.

The feedback from the participants of the basic curriculum that we have issued has been positive. Some of them found our methods and approaches one of the most interesting and innovative ways of delivering an interactive cyber security awareness program. However, there is much room for improvement. The syllabus, course management system and interactive lecture videos could be better prepared, new and more advanced topics could be covered. The scoreboard, topic advisor administration interface could have a better design, a pivotal approach of particularly human-computer interaction and a different language support. Moreover, up to this point, the syllabus has only implemented the IT security awareness issues, and due to the further improvements it will meet the needs of the cyber security field. Due to rapidly changing technologies a synchronized approach could be taken into consideration for updating, upgrading and changing the content of units, modules and courses, in other words the syllabus.

The thesis also describes the results and the evidence from this study points towards the idea that the implementation of the syllabus will improve everyday work and usage of computers, mobile phones, online banking, social networking, and so forth. The paper also indicated an important need for future action. The introduction of the basic security awareness program was successful. We have also seen that the curriculum enables an increase not only in the awareness, but also in the technical knowledge, leadership and socio-technical approach.

We believe that our interactive cyber security program could be implemented effectively in private, public organizations, military, nations, schools and campuses, without a significant degradation in performance. Furthermore, the solution of our course management system could be applied to different educational purposes and awareness programs. It must be noted that future work is already underway or planned by the author.

Acknowledgements

This paper would not have been possible without the support and encouragement of my colleagues and friends. Great thanks to Tartu University and the Tallinn Technical University who enrolled me with a full scholarship in the master of cyber security studies and DoRa9 scholarship funded by Archimedes Foundation.

Additionally, a few individuals and organizations have extended themselves beyond the call of duty and deserve special mention: Jüri Kivimaa supervisor, Dalibor Sojic, K-Net Internet Service Provider - Kumanovo, Photo Cinema Club Kozjak50, English reviewers Ivana Rusevska, Matthew Kelly and many others.

Finally and most importantly, I would like to thank my family, whose love and support has kept me sane, focused, and happy during the writing of this paper, and hopefully in the adventure of launching a new consultancy (CyberSecurity.mk).

9 Appendix

9.1 Awareness Survey Questionnaire

The below survey template is taken from ENISA user's guide: How to raise information security awareness [41].

ICSAP is conducting a study to help determine ways of educating citizens about information security issues. We would appreciate if you could spare 10 minutes to answer a few brief questions regarding information security.

1. How do you access the internet:

   a) ADSL/DSL/Cable/Broadband/Wireless/Satellite

   b) Company Internet

   c) Mobile broadband

2. Where do you use your computer (check all that applies):

   a) Home

   b) Office

   c) Public-access location (school, library, bus, train)

   d) Internet Café

   e) On the move(Notebook, Table PC, Mobile Phone)

   f) Other (please indicate where)

3. Many people define safety as protection from adverse effects. With this in mind, on a scale of one to five, with one being very concerned, and five being the least concerned, how concerned are you about the safety of your information technology assets (computer, peripherals, electronic data, mobile phone, etc)?

   a) 1 - Very

   b) 2

   c) 3 - Somewhat

   d) 4

   e) 5 - Least

4. Which of the following do you think poses the greatest threat to your information technology? You may select any that applies:

   a) viruses and worms

   b) spam and other unsolicited emails

   c) hackers/intruder

   d) fraudulent schemes

   e) malicious software (e.g. spyware)

   f) faulty computer hardware

   g) Other.

5. On a scale of one to five, with one being very knowledgeable and five being the least knowledgeable, please rank your knowledge of the steps that can be taken to protect your information technology assets:

   a) 1 - Very

   b) 2

   c) 3 - Somewhat

   d) 4

   e) 5 Least

6. Do you have any of the following that is in place to protect your computer and electronic data? Please indicate all that apply.

   a) Anti-virus software that is updated regularly

   b) Firewall

   c) Anti-spam filter

   d) Good password practices

   e) Process of regular backup of data

   f) Up-to-date Internet browser with encryption

   g) Locked screen saver on your notebook / mobile phone/ tablet PC

   h) Other (please describe)

7. Which would be the best way to provide you with information on how to protect yourself from potential dangers? In other words, are you most likely to pick up information from the:

   a) Radio / TV adverts

b) Newsletters

c) Online adverts

d) Online training

e) Posters

f) Other (please describe)

Thank you so much for participating in this survey. We plan to use your answers to help us develop information in order to raise awareness of the importance of information security.

Bibliography

[1] *COBIT 4.1.* IT Governance Institute, USA, 2007.

[2] *ATM crime: Overview of the European situation and golden rules on how to avoid it.* ENISA, August 2009.

[3] ISO/IEC 17799:2005(E). *International Standard ISO/IEC 17799.* ISO copyright office, Case postale 56, CH-1211 Geneva 20, Switzerland, 2005.

[4] Spyros Kokolakis Aggeliki Tsohou, Maria Karyda and Evangelos Kiountouzis. Analyzing information security awareness through networks of association. *TrustBus 2010, LNCS 6264, pp. 227-237*, 2010.

[5] Peter Sandilands Andrew Simmonds and Louis van Ekert. An ontology for network security attacks. *S. Manandhar et al. Eds. AACC 2004, LNCS 3285*, pages 317 – 323, 2004.

[6] I. Androulidakis and G. Kandus. Correlation of mobile phone usage characteristics, security awareness and feeling to the monthly bill. May 2011.

[7] Paul Arveson. The deming cycle. website, 1998.

[8] Greg Young Avivah Litan, Don Dixon. *New attacks: device vulnerabilities stand out.* Gartner, 2006.

[9] Tim Berners-Lee. The worldwideweb browser.

[10] J.R. Boyd. *A discourse on winning and losing.* Maxwell Air Force Base, AL: Air University. Library Document No. M-U 43947, Briefing slides, 1987.

[11] Steve Manzuik Paul Guersch Dave Killion Nicolas Beauchesne Eric Moret Julien Sobrier Michael Lynn Eric Markham Chris Iezzoni Bryan Burns, Jennifer Stisa Granick and Philippe Biondi. *Security Power Tools, First Edition.* O'Reilly, August 2007.

[12] Cisco. Cisco visual networking index: Global mobile data traffic forecast update, 2011-2016. White Paper, February 14 2012.

[13] ISO copyright office. *Information technology, Security techniques, Information security management systems, Overview and vocabulary.* INTERNATIONAL STANDARD ISO/IEC 27000, 2009.

[14] From correspondents in Seattle. Microsoft issues biggest software patch on record, 14 October 2009.

[15] American Heritage Dictionary. American heritage dictionary entry for back up, 2009.

[16] T. Dierks. The transport layer security (tls) protocol version 1.2, August 2008.

[17] Don Dixon. *How to mitigate information loss on MFPs.* Gartner, 2006.

[18] The Economist. Getting the message, at last, December 2007.

[19] UCLA Engineering. How to protect against malicious software, N/A.

[20] Jon Erickson. *Hacking: The Art of Exploitation, 2nd Edition.* No Starch Press, Inc., 2008.

[21] Peter J. Grant et al. *Hype cycle for printing markets and management.* Gartner, 2005.

[22] Ganapathy and Iftode. Rutgers researchers show new security threat against smart phone users, 22 February 2010.

[23] Government Accountability Office (GAO). *Protecting Personally Identifiable Information.* Report 08-343, January 2008.

[24] N.S. Gill. The roman military system, 1997.

[25] Joan Goodchild. Social engineering: The basics, February 2012.

[26] Kimberly Graves. *CEH - Official Certified Ethical Hacker Review Guide.* Wiley Publishing, Inc., 2007.

[27] SANS Institute. Developing a security-awareness culture - improving security decision making. *SANS Institute InfoSec Reading Room*, 2005.

[28] ISECOM. *Hacking Explosed Linux: Linux Security Secrets and Solutions, Third Edition.* The McGraw-Hill Companies, 2008.

[29] ISO. *ISO/IEC 27002:2005.* ISO copyright office, Case postale 56, CH-1211 Geneva 20, Switzerland, April 2008.

[30] Kaur Kasak. Practical exercises for information security courses. Master Thesis, 2009.

[31] Jüri Kivimaa and Toomas Kirt. Evolutionary algorithms for optimal selection of security measures. *Legitimate Defenses Against Dangerous Archenemies*, 2011.

[32] Bob Lord. 1937 enigma manual by: Jasper rosal - english translation. 1998-2010.

[33] Guillaume Lovet. 40th anniversary of the computer virus, 14 March 2011.

[34] Command Five Pty Ltd. Advanced persistent threats: A decade in review. June 2011.

[35] SC Magazine. A brief history of internet security, September 2009.

[36] Chris McNab. *Network Security Assessment.* O'Reilly, March 2004.

[37] Julian Mehnle. Sender policy framework: Introduction, April 17 2010.

[38] Apu Kapadia Joshua Haines Michael N. Gagnon, John Truelove and Orton Huang. Isarcs 2010, lncs 6150: Towards net-centric cyber survivability for ballistic missile defense. *Springer Verlag Berlin Heidelberg*, pages 125–141, 2010.

[39] Rashid Bin Muhammad. History of operating systems, N/A.

[40] European Network and Information Security Agency. *Secure printing*. ENISA, April 2008.

[41] European Network and Information Security Agency (ENISA). A users guide: How to raise information security awareness. Nov 29, 2010.

[42] OCDE. *Malicious Software (Malware): A Security Threat to the Internet Economy - DSTI/ICCP/REG(2007)5/FINAL*. Organisation for Economic Co-operation and development (OECD), June 2008.

[43] United States Joint Chiefs of Staff. Joint publication 3-13: Information operations, February 2006.

[44] PCI. *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures*. Verison 2. PCI Security Standards Council LLC, October 2010.

[45] Prasanna Ramakrishnan. Information security management systems. *CISSP*, 29.10.2003.

[46] Dimensional Research. The impact of mobile devices on information security: A survey of it professionals. Research, January 2012.

[47] Uri Rivner. Anatomy of an attack. Blog, April 1 2011.

[48] Jason E. Samulaitis. *A Guide for Best-Practices When Using Your Computer at Work*. Pembina Trails School Division, 2005.

[49] Chris Savarese and Brian Hart. The caesar cipher. *Trinity College Department of Computer Science*, 04 2010.

[50] Grefory M. Schechtman. Manipulating the ooda loop: The overlooked role of information resource management in information warfare. 1996.

[51] Ed Skoudis and Tom Liston. *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall, 2005.

[52] Sophos. Security threat report 2012. PDF Report, 2012.

[53] sourceDaddy.com. Wireless lan implications.

[54] Lance Spitzner. How to build an effective information security awareness program. October 2010.

[55] Dafydd Stuttard and Marcus Pinto. *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*. Wiley Publishing, Inc., 2008.

[56] Predrag Tasevski. Password attacks and generation strategies. *Tartu University, seminar work*, May 2011.

[57] Verizon RISK Team. 2012 data breach investigations report. 2012.

[58] TechTarget. Definition: Social engineering, March 2001.

[59] TechTarget. Definition: Physical security, December 2005.

[60] Kevin Tyrrell. Sans institute infosec reading room: An overview of wireless security issues. 2003.

[61] PricewaterhouseCoopers LLP (UK). Information security breaches survey 2010. 2010.

[62] Von Solms R. Vermeulen, C. *The information security management toolbox - taking the pain out of security management.* Information Management & Computer Security 10(3), 2002.

[63] John Viega and Gary Mcgraw. *Building Secure Software: How to Avoid Security Problems the Right Way.* Addison-Wesley Pro, 2002.

[64] The White House Washington. The national strategy to secure cyberspace. February 2003.

[65] Ken Weilerstein. *What IT Asset Managers Need to Know About Managing Office Print Before It Falls Into Their Lap.* Gartner, 11 November 2005.

[66] Mark Wilson and Joan Hash. *Building an Information Technology Security Awareness and Training Program, Computer Security.* NIST Special Publication 800-50, October 2003.

[67] Susan Young and Dave Aitel. *The Hackers Handbook: The Strategy behind Breaking into and Defending Networks.* AUERBACH PUBLICATIONS, 2004.

[68] William Zeller and Edward W. Felten. Cross-site request forgeries: Exploitation and prevention. October 2008.

Abbreviations

ACK	Acknowledgement field
APT	Advance Persistent Threats
BMD	Ballistic-Missile-Defence
BSD	Berkeley Software Distribution
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CMS	Course Management System
CSRF	Cross-site request forgery
DKIM	Domain Keys Identified Email
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denail-Of-Service attack
DoS	Denial-of-Service
ESSID	Extended Service Set ID
FAQ	Frequently Asked Questions
GSM	Graded Security Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems

ISMS	Information Security Management System
ISP	Internet Service Provider
LMS	Learning Management System
MAC	Media Access Control
NGO’s	NON-Governmental Organizations
OODA loop	Observing, Orienting, Deciding and Acting
OS	Operating System
PDA	Personal Digital Assistant
PDCA	Plan, Do, Check and Act
PGP	Pretty Good Privacy
PII	Personal Identifiable Information
PIN	Personal Identification Number
RSA	Public Key Cryptography Algorithm and security firm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIM	Subscriber Identity Module
SPF	Sender Policy Framework
SSD	Solid-state Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronize sequence numbers
TCP	Transmission Control Protocol
TCP/IP	Internet Protocol Suite
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus

VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
XSS	Cross-site scripting