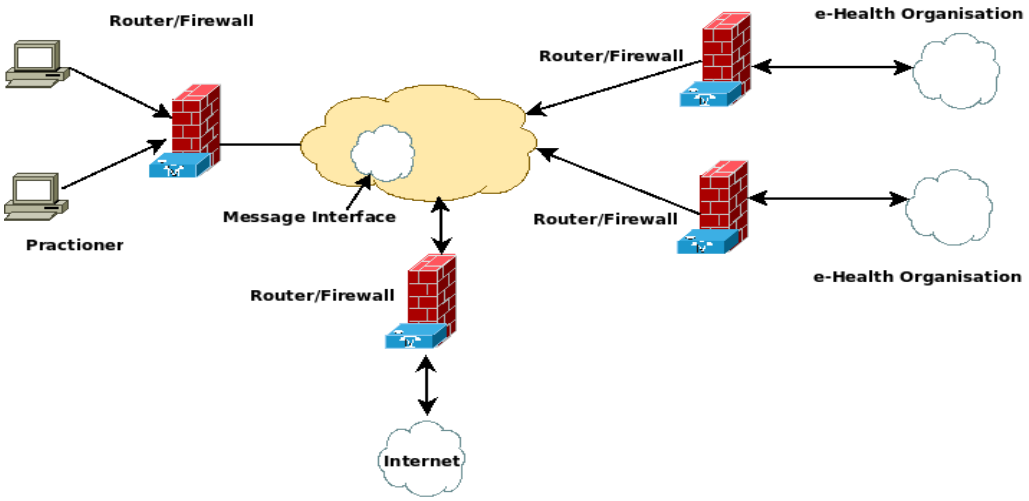
UNIVERSITY OF GOTHENBURG




# e-Health Security Issues and Solutions

*Master of Science Thesis*

NAJIB ZIAIE

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
Göteborg, Sweden, September 2013

**Abstract**
The aim of the thesis is to give an understanding of the current situation and its security issues within the e-Health institutions. Following the analysing of current protocols and administrative concepts, an overall approach is given, of how security can be implemented, maintained, measured and ensured. This is achieved through the usage of standards like ITIL, ISO 27001, an management approach, which fills the gap of the mentioned standard introduced as top down approach. Later on the method called, Penetration-Testing will be presented which measures the current state of security level of an organisation. By developing these concepts, the focus lie on use cases of e-Health institution.

**Acknowledgements**
My first thanks goes to Arne Linde for providing guidance and being my supervisor, the University of Gothenburg and Chalmers for providing learning resources and for nominating me to spend the last part of my M.Sc. at the University of Birmingham. Many thanks also for the Professors from the University of Birmingham, especially to Guilin Wang, who gave me specific advice on security related questions.


Examiner: Arne Linde

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Göteborg Sweden

1 This thesis was presented in September 2010 because of administrative reasons it has been resubmitted in September 2013. There are no differences between the two versions, beside the first two pages.

# Contents

# List of Figures

bindingoffset=30mm,top=24mm,textheight=245mm,textwidth=160mm,heightrounded,right=27mm,head=1

# 1 Introduction

During the last twenty years modern technologies have changed and influenced our attitude and way of thinking. The new generation is growing up with social networking portals and more and more see this as an essential part of the daily routine. Moor's Law published in 1965 (Pre09) by the Intel entrepreneur, Gordon Moore who claimed in his paper that the numbers of transistors which can be placed inexpensively on an integrated circuit will be doubled approximately every two years. Indeed, he was right with his theory, also in the area of medicine, we can see traces of new development procedures. Beside of new electronic health devices which makes new forms diagnostic methods possible, the information processing opens also new forms of new knowledge based representation of data which will be used to develop unimaginable opportunities in the future.

Today we are facing and moving from an industrial age into information age, for example our postal system is being very much replaced by e-Mail. Our telephone system is now being replaced by Voice over Internet Protocol (VoIP), and buyer and consumer behaviour, is influenced by e-Shopping. Same happen in the area of healthcare, where we are moving to the term of e-Health. Many governments worldwide have launched different approaches to design and develop solutions to support improvements in care. To reach this objective, a strategy is needed, where the focus is mostly based on the use of information communication technologies, short ICT. Through the introduction and usage of such implementations, the aim is to bring cost savings or cost reductions and better process workflow in e-Health organisations, like hospitals. The Healthcare sector is an industry with different stakeholders; governments, practitioner, insurance companies, patients/clients and family members, chronically ill patients, private patients, home care and so on. However, building up and connecting networks, with the idea of exchanging data, between different health organisations and stakeholders is challenging and can be very complex. It is on the other hand clear, that this step brings a lot of improvements for patients and health professionals involved in care and management, as well as for those organisations needed to be profitable[1], considered from the economic point of view. As in (Zia07), stated many solutions are useful, however security threats (Mil09) are on the rise. Hospitals and other health organisations, where confidential data is stored must be prepared to face the problem of computer theft, fraud and other threats in their IT systems. The idea of leaked IT systems and the possibility, that an attacker can gain access to someone's electronic health record (EHR) 2.2.1, for instance, could be crucial. The conficker worm (Mil09), which was one of the big threats in 2009, infected several hundreds machines and critical medical equipments in the US. A survey points out (SAN09) that application security exceeds OS vulnerabilities, see figure 1 . Even viewing an adobe PDF file can be used[2] to infect users (II10). All this

[1] Especially private hospitals.
[2] Zero-Day-Exploit.

backs the assumption that a research into this direction is needed. Specially then, since the application used within e-Health institutions are not secure. They are made to just do their purpose.[3]

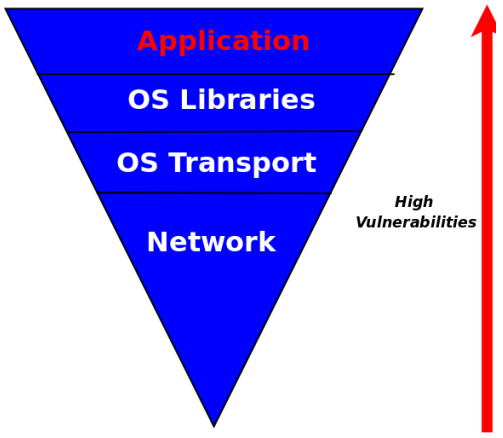



Figure 1: Application vulnerabilities on the rise

Studies like (Zia07), (Lou99) claim that in the near future the e-Health branch will belong to one of the biggest sectors in our economy. This assumption is very much based on the theory of the Kondratiev Waves, see figure 2. This waves are also sometimes called as super cycles. If we consider past developments, we can summarise the strength of each economic growth through the cycles of Kondratiev (Lou99). Each cycle or wave represent a period of time where the main economic strength is based on that industrial invention. For example, the invention of the steam engine opened the era of mass production of goods. The introduction of IT on the other hand, was responsible for global economics.
If we start comparing the investments in the health sector we can distinguish, that about 3% of the budget is spent for IT, in other industries investments are much higher, they spend between 5% and 7.5% of budget available(Zia07). How important the health sector is, shows the fact that around 4.2 jobs were created alone in Germany, which is around 12.2% of the gross domestic product (GDP), corresponds to 260 Billion Euros. The 4.2 million jobs have also been the largest sector of the economy, furthermore the health care industry is growing much faster than the economy as a whole.

## 1.1 Thesis overview

The thesis is divided into mainly two parts. During the first part, I will give an overview about the current state of e-Health regarding present situation. This includes the intro-

[3]This claim, was possible after researching about the companies involved in producing software applications for e-Health institutions, such like hospitals. Inside those companies IT security professionals could not hardly be found.

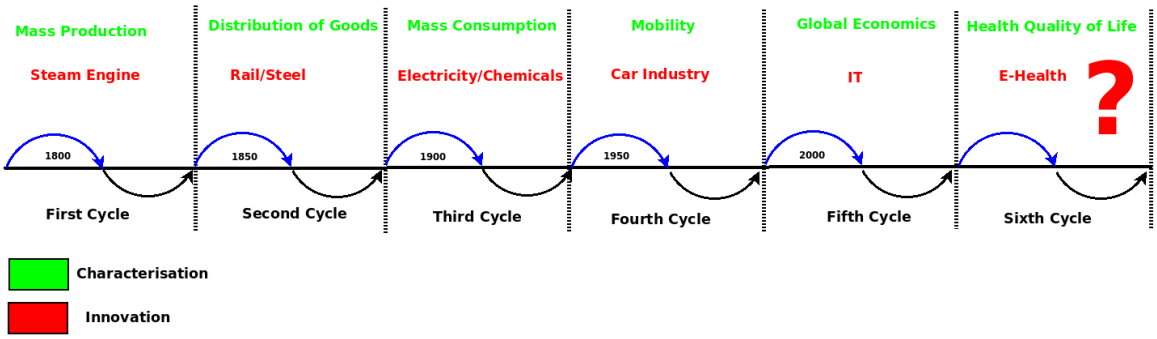



Figure 2: Kondratiev Waves

duction of a hospital environment as a typical e-Health institution. It follows with the discussion of typical protocols and assets which need to be secured in way and on the other hand should be shared between the stakeholders. Hereby, it is important to share those assets in a secured, efficient manner. During the next sections a discussion about problems and solutions are presented. Later on, the topics of useability, e-Health and security are introduced. During the last sections the idea of how IT security can be made manageable and a testing procedure in order to measure the current level of security will be presented.

# 2 Present e-Health Situation

Before talking about the present e-Health situation, the term e-Health should be defined. It should be added that there is no unique definition for the term, however the definition of Eysenbach(Eys09)describes it best:

"e-Health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterises not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology ."

As the definition describes, e-Health has different areas, one such area is called telemonitoring. We talk about telemonitoring, when practitioners treat their patients from distance by using ICT equipments. With other words, this can be achieved by using electronic devices, or telecommunication devices to monitor the patients health state. Such home monitoring systems are very usefull for chronically ill patients, for diagnosis purposes. One such device is a pacemaker which is produced by companies involved in the growing e-Health branch. Devices for home monitoring system services are used, by using the internet. The idea of using the internet to treat mainly patients who are chronically ill has many advantages:

For the patients it is an advantage, since there is a phenomenon which is called "white coat hypertension", the data taken through telemonitoring is more reliable, also for the doctors it is convenient to have the latest healthcare data, which results in better treatment quality.
An advantage for physicians and hospitals could be efficiency in their daily workflow, since electronic documentation becomes essential, thus recent technologies can obviously assist them. Beside the fear of usefullness some may have, studies showed, especially chronically ill patients visit their doctors almost weekly and since the introduction of the ICD10 system 2.4 practitioners earn very less when they treat patients who are chronically ill. To sump it up telemonitoring system can actually benefit both at the same time, doctors and patients. Another big advantages brings the use of such systems, when patients are located in areas where practitioners are rare, like villages, hence the system helps to link patients and doctors, even when they are separated over a long distance. Nevertheless, patients feel in their homes much more comfortable than patients in hospitals. It is also more safe, since bacterial infections inside hospitals is on the rise (BBC09).
Every system has also some drawbacks, in this case, patients could lose the faith in treatment, since practitioners usually spend a few minutes for diagnosis, using telemonitoring systems could result in more misunderstanding and in a disturbed relationship between doctors and patients. In this case it must be assured that patients are individually questioned if they agree with the therapy method from distance.

## 2.1 e-Health Problems

Nowadays e-Health institutions have to face many problems within their organisations the challenge comes mainly from government agencies who somehow decide over regulations, from the stakeholders within the organisations and from the patients who have specific rights assured through government rules. One important issue, is the fact, that most of the institutions can not use the benefits of nowadays technology improvements given. One such example is the case of efficient workflow optimisation. Through different methods, like RFID usage, scheduling theories, expert system and specific standards which efficiently can be used within other branches like banking, logistics, somehow the usage of the "best practises seems" to take a long period of time till it is implemented or considered inside e-Health institutions. There are still inefficient pathways used, one example is the case when patients x-rays or other data need to be transmitted to other specialist. In some hospitals this is still transported through a taxi driver who brings the patients data saved on a CD to the destination wanted. Inefficiency, is a term which can be eliminated by the possibilities the institutions have, these should be encouraged by the stakeholders and this seems to be a big challenge in the near future. For the importance of IT security most e-Health institutions does not take the issue too serious, since they often become serious when incidents happen, on the principle action needs reaction.
Major problems occur, when intruders have large budgets, since it becomes more difficult

to handle intrusion as the budgets increase. Those individuals with the aim of using various techniques to access valuable data through:

- Reverse HTTP tunnels
- ICMP backdoors
- Sniffers

are nowadays organised groups, who specially middle sized companies and health institutions should fear.
This activity introduce the field of e-Crime, where a computer network is the source or the place of the crime. e-Crime is very difficult to detect, since attackers can strike from different locations, from thousands of kilometers away. The figure in 3 describes the impact of e-Crime.

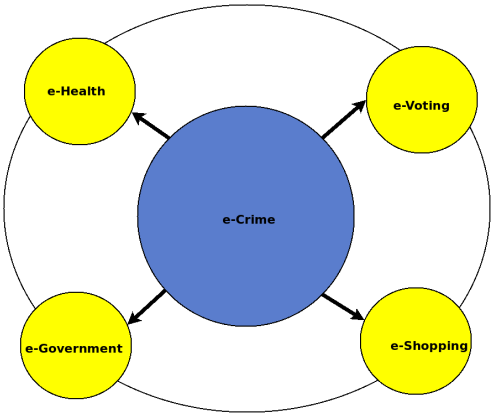



Figure 3: e-Crime impact

Why software is often insecure has different reasons. One reason is that applications tend to be written in isolation. The bigger picture of the OSI shows applications on top of the operating systems which on the other hand is connected through networks operating system to file systems. They are all programmed with the help of communication protocols, such as HTTP, FTP, Telnet, TCP, IP etc. These protocols have all one thing in common, in the role to establish a connection, no security mechanisms were specified. The figure in 4 gives an overview of the origin of HTTP attacks.

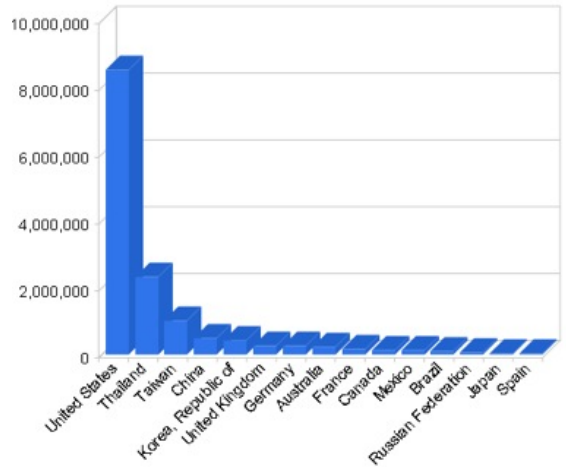



Figure 4: HTTP Attacks by Source, according to SANS

Considering an hospital as a typical e-Health organisations, we can say that it is characterised by a decentral workflow environment, where the processes are complex with no standard software to coordinate all these processes. Depends on political and legal decisions, which make it more complicated, it often happens, that patients complain:

"I really needed just a prescription and have been waiting for half an hour. They told me I just could pick it up."

On the other hand through the introduction of Diagnosis Related Group system (DRGs), as a result of this hospitals with low operating costs and high productivity perform better than other houses, hence some houses may get financial difficulties and the pressure between institutions will increase. In order to be profitable it must be assured, that patients are satisfied. Studies showed that more and more people choose supplementary private insurance companies to get the best treatment.
That the employees, nurses, doctors are satisfied is another big challenge, in Germany as an example, the doctors in the clinics have to work long hours, and as a result they migrate to Sweden, Switzerland, which results in shortage of doctors. Another problem they have to face, is the problem of the increased cost pressure in health systems. The big challenge however will be from the perspective of an hospital:

How can we efficiently coordinate the processes under these circumstances and ensure security?

To solve these problems mentioned a fundamental change must be proceed. These changes and recommendation will be given during the upcoming sections, where the focus will be on the security part.

## 2.2 Case study: Hospital Environment

To plan, maintain and regulate a Health Information System (HIS), there is a need of an architecture. The architectures gives an an insight about the overall structure of the HIS, with the separation of modules from which it consists. The whole concept of an HIS can be described with the help of 3LGMg meta model. Most university hospitals worldwide use the 3LGM management model (WT04). As the name indicates, it consist of three layers, see figure 5:

- **Domain Layer**
  In this layer the main duties of an hospital is modeled, for instance during the arrival of a patient the medical history need to be accessed, so that no mistakes towards medication can be made. These type of information is represented in entities, which can be maintained through access class, where the attributes regulates its access type.

- Logical Layer
  At the logical layer application components, the assurance of communication and storage are the main task of this layer. The application components are controlled by application programs.

- Physical Layer
  The physical layer is a set of physical processing components, which can be any physical device inside the hospital, such as telephones, paper-based patients records (asset). They are connected through wires and are based on network protocols, like TCP/IP, HL7, DICOM etc. Since different networks may be connected internally the connection of RIS and hospital administration system can be mentioned as another example.

To sump up, modelling hospital information system can be described through 3LGM in a static way, where an hospital information system (HIS) is the sum of all activities and processes involved in an hospital, with the help of IT and without.

### 2.2.1 EHR/EPR

In a provider based electronic medical record typically medical information about patients is recorded. This record is the fundamental tool which every doctor need to read, write, in order to give the best care each patient should get. Medical records are important, since from individual healthcare provider to small physician office practices, to large hospitals, healthcare insurance companies, without patients data like billing data, insurance claims, they simply can not work. Personal records of hospitals, like numbers of birth, immunisation and death, for instance are important for state control agencies. The care suffers when patients data is not at the right place or is lost. It must be assured, that everyone who has the right, can access the record, in an efficient manner, where no waiting time or a deadlock situation can occur. For a while these records where maintained not

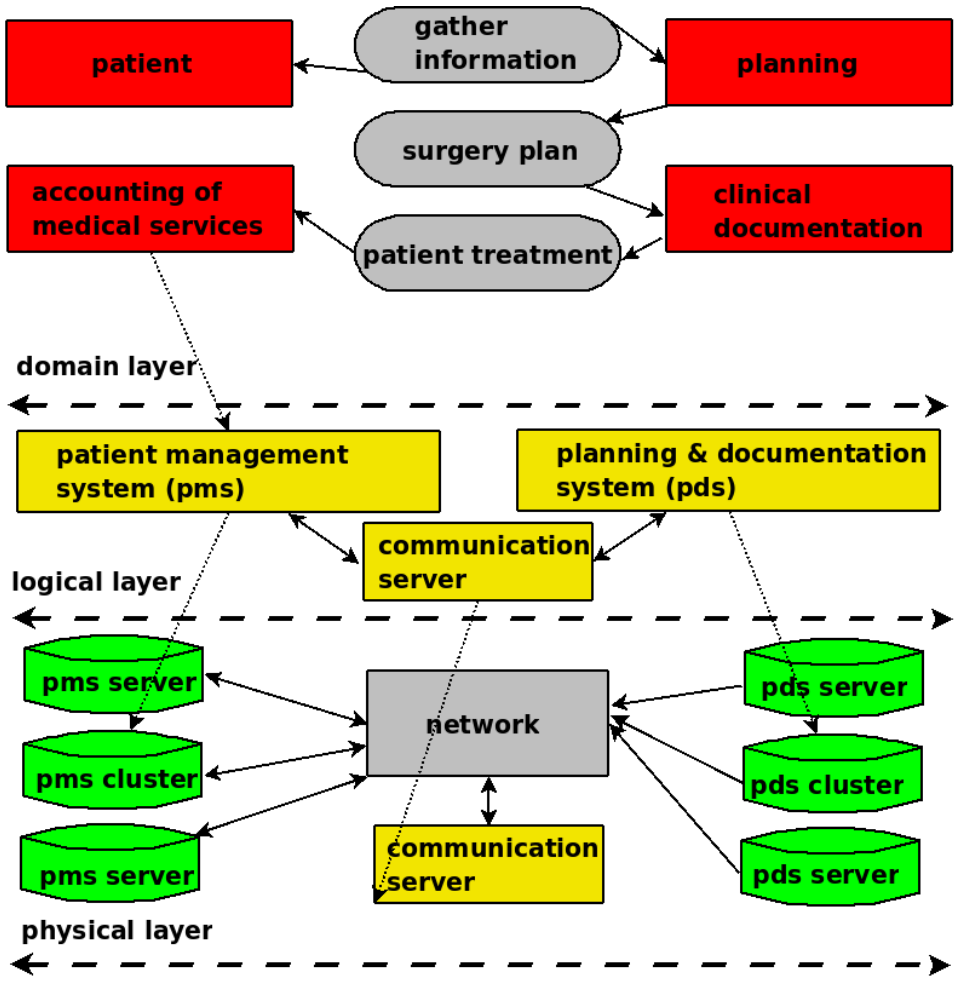



Figure 5: Hospital Information System (HIS), 3LGM model

electronically and in some hospitals health data is still maintained by hand by writing it down and are passed over, whoever requested it. The drawback of this convential method is, however, that deadlock situation can occur and last but not least the explosive raise of costs. Many university hospitals still use the paper version, but most of them are planning to adjust their workflow to introduce it electronically. In German hospitals 6 million pages of documentations are produced annually. Regulation rules makes it much more, since each university have to keep the data of each individual patient for at least 30 years accessible. This is a great challenge for health institutes. According to a survey during the thesis research the following advantages are given to introduce EHR's.

- Multiple users can access the health data simultaneously
- Access to patients data is given in an efficient manner
- Different group of individuals, for example doctors or nurses can view individual views on the patients record
- Searching for specific data can be valuable for future patients, for example which health threat may be risky or which treatment is best
- Losing the records cannot occur (if appropriate technical solution exists)
- Cost savings

The Electronic Patient Record (EPR) is a set of data in which medical treatments are recorded. It is very common that different EPR's exist. The EHR is a record in which all information and medical data from EPR's are included.
The patient has the right to access his medical history, this is part of the law in many European countries. The patient can also take copies of the documention, if desired. It is a difficult task for the hospital information manager to decide which documentation venturer, from a variety of existing solution in the market, is suitable for his organisation. However, the likelihood to prioritise lower the security issues might happen more often than thought. A lot of managers do not actually have a degree in IT Security, or not even bring an IT background. This is fatal to the whole organisational structure of an e-Health institution, which is highly risking a lot of trouble.
Having access to medical records through IT opens possibilities like cost reduction and improvements in care. Although there are big challenges towards the threats and security issues, which we are facing today. Expansion of new efforts are necessary before the problem is resolved and benefits are realized by the stakeholders.

## 2.3 PACS

PACS stands for Archiving and Communications System and is used for storage, viewing and manipulation of radiological images. The functions includes the following:

- Acquisition devices
  Devices which convert the analog output from imaging to digital formats.

- Storage
  Archiving solutions which are short term or long term based.

- Communication PACS requires high speed connectivity to transfer images from one machine to the one needed. The transmission of images is based on the protocol called DICOM.

- Specific software
  Specific software is need to interact with PACS systems. Image viewers must be, for instance installed on diagnostic workstations, which are mostly hig-end systems with high resolution etc.

- Image Compression
  Image compression is another important issue which is used within PACS, the large amount of file size makes it impossible to keep the size once the image is taken, thus compression like JPEG 2000 is used to minimise the file size up to 10:1 without significant loss of clinically relevant data.

## 2.4 Challenge: Data Standards

Hl7 and DICOM are probably the most important protocols used within the hospital environment. These are used to exchange healthcare specific data between the different entities of the e-Health sector. In detail:

- HL7
  Hl7 stands for Health level 7, which refers to the application layer of the OSI layer model. Originally, Hl7 was a team of individual programmers to help standardise the communication channel of incompatible healthcare applications. HL7 is based on XML and therefore fits perfectly to exchange the data of an clinical information system and to use it as a documentation schema for EHR/EPR.

- DICOM
  DICOM is a standard introduced by the industry which is used for transferring radiological images between different hosts. DICOM was set up by National Electrical Manufacturers Association (NEMA) and by the American College of Radiology (ACR).

As mentioned above HL7 is the standard for the exchange, management and integration of healthcare information. The combination of both can benefit any e-Health organisations.

**SNOMED-CT**
SNOMED-CT stands for Systemized Nomenclature of Medicine-Clinical Terms, it is a

systematically collection of the terminology of medical information such as diseases etc. The main aim of SNOMED-CT is to give a standard terminology of precise recording of clinical information which has an inherent structure. IT has about 800.000 terms which describes about 300.000 concepts. SNOMED has his origin in SNOP which stand for Systematized Nomenclature of Pathology. The first version was released in 1974 and many different updates followed from then. Since April 2007 the rights of SNOMED-CT lie on the International Healthcare Terminology Standards Development Organisation, (Org10) (IHTSDO). SNOMED is used in many countries, translated into many different languages like Spanish, German, French, however, only the English and Spanish version is under certain conditions free of charge. The design of SNOMED-CT is based on descriptive logic, according to (SNO10), the components are:

- Hierarchies
  Has 19 higher level hierarchies, with each of them divided in sub hierarchies.
- Relationships
  Concept either within or throughout the hierarchies.
- Concepts
  Basic unit, each concept has an unique numeric code, unique name and descriptions.
- Descriptions
  The descriptions can be terms or synonyms assigned to denote a special concept.

In addition to the preferred term each concept has a fully specified name. For example the concept provided for the concept identified as 22298006 are:

Fully specified name: Myocardial Infarction (disorder)
Preferred term: Myocardial Infarction
Synonym: Cardiac infarction
Synonym: Heart attack
Synonym: Infarction of heart
Synonym: Infarto de miocardio

### ICD-10

ICD-10, which is an international standard, stands for International Classification of Diseases. The standard maps uniquely diseases into codes by especially trained coders inside the clinical department. It is also internationally known, but different versions exists in different countries.
In comparison, SNOMED-CT is used in the whole healthcare domain[4]. The benefits of its use are:

[4]Not limited as use case

- it allows to effectively communicate across clinical domains
- it has the best coverage of clinical concepts out of all existing systems
- it is the only terminology which support the development of clinical knowledge base One drawback could be that since the standard is very complex, introducing over night is impossible.

One important issue is the case of providing security over the patient data. These are normally covered under the Health Insurance Portability & Accountability ACT (HIPAA). However, unauthorised access to patients data are difficult to monitor(Hos09).

Numbers & Facts
Another challenges comes up since the data must be saved for at least three years in some countries maybe more. The following overview shows what kind of data must be saved or processed within and to e-Health organisations each year.

- Sales about 500 million EUR
- 7000 Employees
- 1600 Beds (efficient allocation)
- 55000 incidents and cases each year
- 400.000 outpatients and visitors per year

Each year about:

- 250000 discharge summaries
- surgical reports
- 800 000 clinical chemistry findings
- 200.000 radiological findings
- 20.000 pathology findings
- 100.000 microbiological findings
- 6 million pages of medical records,

data which must be allocated to areas within and outside the organisation. The amount is approximately 2 terabytes big.

## 2.5 e-Health Solutions

The following sections tries to give a summarised version of the purpose and aims e-Health organisations may have and the strategy they are following.

### Aims & Objectives

Most of the solutions purpose try to benefit the workflow within e-Health organisations, like healthcare services. Introducing electronic health smart cards is one of the method to bring down cost, higher the efficiency rate and benefits healthcare services in general.

### Strategy followed

Some strategy is based on an electronic patient file, which should last for a long time. This file is unique and is created for each patient. This is the strategy in Switzerland. To achieve these goals the stakeholders in all areas in Switzerland need to agree on legal and technical issues, regarding safety and to ensure compatibility. Beside this the implementation is approached from top to down of the organisation.[5] Some others believe in a central server, where medical records are storaged, so that the care givers know exactly the whole medication history. Interaction in this processes by patients are welcomed, since this belongs to the project goals of the government. Services like real time information will be accessible through online services. The time plan for project closure is seen for 2015. The strategy of Switzerland is compareable to the strategy of Germany where similar objectives are set for the project, like e-Prescription, e-Referral letter etc. The National Health System (NHS) strategy in the UK started to evaluate the structure from the 90's where they came to the conclusion, that the systems were old and the integration of new systems impossible. Later they formulated aims to bring up a system which supports the following:

- Security and confidentiality
- NHS network (NHSnet Topology) which opens information sharing
- System integration, data uniqueness
- A number which represents each patient (which Sweden already have)
- Evaluate data and manage information from the daily task

The strategy was changed during the years and in mid 2000 some other aims where included. The plan was to:

- The NHS network should be connected with all practitioners (GPs)

[5] The drawback is that useability can not be assured and that the risks of project fail increase.

- Patients should be able to view their EHR/EPR
- e-Booking system for outpatients, regarding appointment
- e-Prescription

However, the objectives described could not be accomplished so far, the time plan set were not possible to hold and all the other reason are somehow the same like in other proposed solutions in Europe. The British Medical Association for instance, suggested practitioners (GPs) should not sign the agreement for NHSnet, because of security reasons, in which later only 1/3 signed the agreement. Other issues were proclaimed confusion over roles, slow network and lack of support for NHSnet. These strategies are more and less the same for each country, see figure 6, beside some minimal differences. The differences lie in the idea of how the implementation should be approached, if a smart card solution works best or any other. Regarding the time plan, as in most big projects, the complex situation

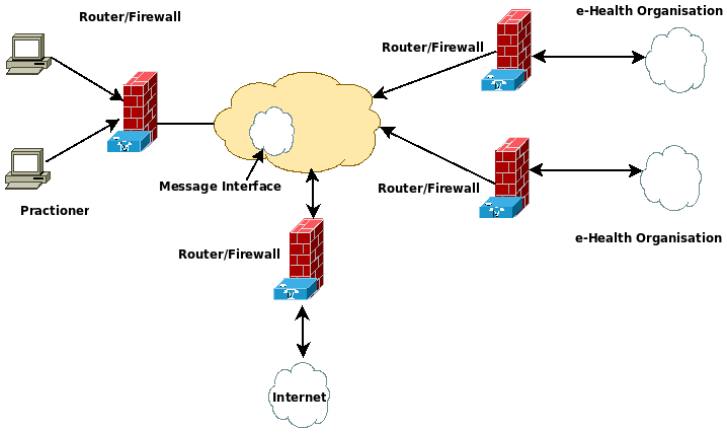



Figure 6: Typical e-Health solution

makes the project to be late. The reason for this is because of the complex interactions and dynamics of change by stakeholders, government regulations, laws in addition to false goals set during the planning phase which make projects late.

### 2.5.1 Case study: German Health Card

The German health card is different in comparison to banking, or other smart card solutions, where the interaction with data or access is limited. The electronic health card belongs to the first project ever, which regulates access to specific medical data, only then when the user, in this case the patient allows it. It can be compared with a rented safe inside a post office. This is possible because the architecture makes use of a two way smart card system. The patient has its own unique smart card, also his doctor has his smart card. Only when both cards are used at the same time an encryption is possible and the

data can be send out to different other institutes, like hospitals, to the patients insurance company or to a specialist within the medical field.
Another important issue is, that each patient has the right to decide on the use of his medical data. Theoretically a patient even can deny to accept that his medical history is saved electronically[6]
The processor of the smart card is compareable to computers from the beginning 1980s, however the whole functionalty is pressed on 25 square millimetres semiconductor material. The processor fullfills mainly two functions:

- First, it assures authentication, where the user set a specific identification number like a PIN code of his own choice. This PIN code is then saved in encrypted form on the chip. After this, no one can access the data without the correct PIN code.
- Second, it assures an encryption schema, where all medical data of a patient is cryptographically secured. Once encrypted it is theoretically infeasible to crack the encryption to reveal the data. Encryption is based on symmetric and asymmetric encryption, namely RSA and in the future epileptic curves (ECC).

The following figures 7, 8 describe the functionality of encryption and decryption:

**Encryption**

1. Data arrives at the connector
2. A random unique key is generated and the data is encrypted with that random key (symmetric)
3. Secret key is encrypted with the public key of patients smart card
4. To make sure the data belongs to the patient and the doctor signed it, a certificate is attached
5. All data (encrypted medical data + encrypted key) is ready to send.

**Decryption**

1. Patients and doctors smart card must be inside the reader
2. Encrypted data arrives at connector
3. Only secret encrypted key is send to patients smart card, the processor decrypts the key and send it back to the connector
4. Now the medical data can be decrypted
5. The private key of the smart card never leaves the chip.

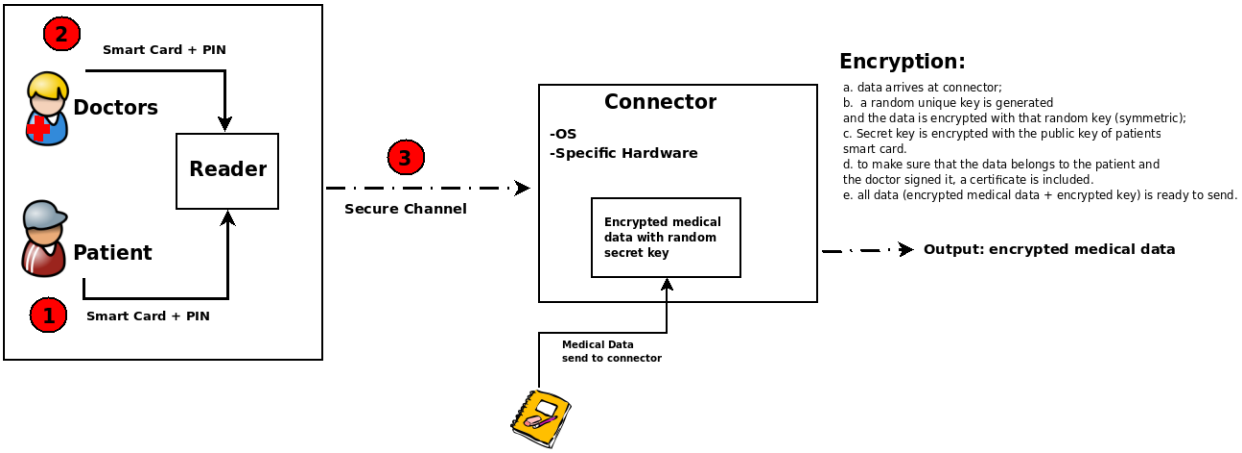



Figure 7: Medical Data Encrypted

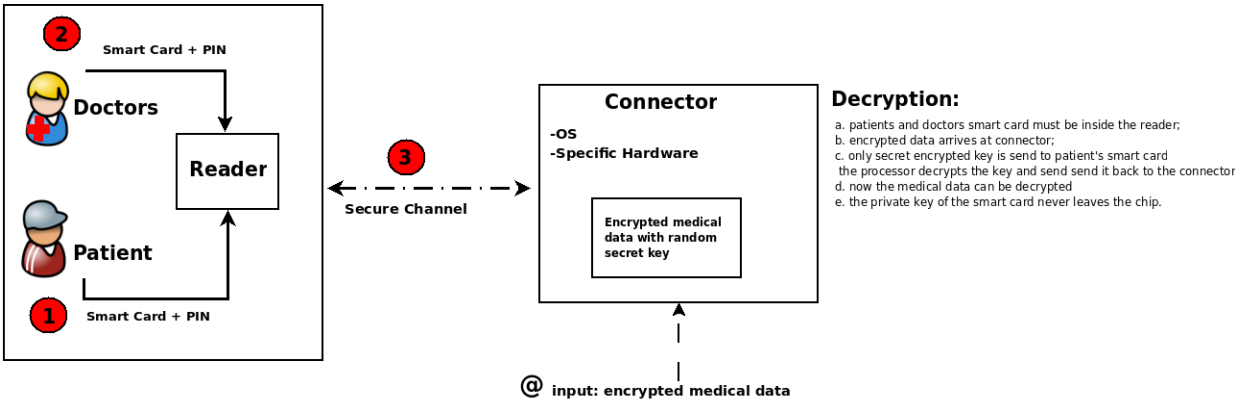



Figure 8: Medical Data Decrypted

Problems which make its use insecure or inconvenient:

- Before the first choice a specific PIN code is set by the patients, here the problem of a weak password may occur, Joe accounts, 1234 could be a password!!
- Especially elderly people tend to forget their password, this could make its use inefficient
- Only when each patient and the doctor has typed his password, he can treat the next patient, results in bad effenciency
- New equipments results in more costs

How smart cards can be proofed insecure or unsmart, gives us the example of the government plans to introduce e-Passports at border control. With the method of (Jee09) used THC has discovered e-Passport weaknesses in different countries. The vulnerability lie on the fact that the reader of the e-Passport can not recognise false e-Passports. Through a modification of the chip, it was easily possible to use a different name, address, picture, nationality and other credentials.

Another example of broken smart card solution is the London Oyster card. The Oyster card is used as a e-Ticket system for public transport within the Greater London area. Its weakness is that copies of the Oyster cards are easily possible. Sniffing the data and clone the RFID chip was sufficient to use the transportation for free.()

### 2.5.2 Conclusion

As previous smart cards solution were broken the question of how to find a vulnerability and exploit it, is probably a matter of time. Even when the smart card solution is theoretically build in with strong cryptographic protocols, such a system can be still broken. Typically in every system, its security level is given by the weakest link, in my findings, it was the user who may need prober time till awareness comes into his mind, other stakeholders included.[7]

# 3 Useability vs. e-Health

As the German patient card proved bad useability in big IT projects can make the whole project fail. Since the interaction of patients in e-Health solution is the fundamental part

[6] German law: 291 a Abs.3 Nr4 SGB V.

[7] Even awareness may sometimes not help, I have never thought that one day someone can use my credit card for skimming purposes. I do not know for sure but believe it happened while being on a trip to Dubai, where I used a prepared ATM. The ATM was such equipped that no links to any bank were established, it stands in midden of the grocery store and after typing the pin, it just printed a label stating "Service Unavailable". Countermeasure, type on unknown ATMs on the first try a wrong pin, when it is accepted, congratulations you tricked the skimming machine.

of any implementation, it is very important to understand the needs of the users. Before implementing an IT-Solution in an hospital environment, the design and the usability of the system should be taken into account. This indicates for instance the question:

Who is going to use the system?

which must be answered in advance, before introducing such systems. Typically the staff like nurses, doctors and different other employees have mostly rare knowledge about IT or they just do not have the time since, their main duty is namely the care itself. IT is hence important, that IT systems should be implemented in a way, that it assists, helps and encourages the staff in their daily work and to not make workflows more complicated than they already are. In the past most of the IT implementation resulted in more work for the staff, this is one reason why some may believe that IT solutions can not help in general, hence they lost faith in IT implementations. From this background, future implementation should assure every detail is according to the user groups.
Useability must consider the society in its form, surveys of how people interact from different backgrounds and age can help to find better useability solutions. According to such surveys the decisions should be made. Sometimes timing can be an important key for success or fail, one example, is surely the build in solution of TV and Internet. During the end of 90's and beginning of 2000 the companies tried to sell their great idea, but it is still not common to have such a device inside homes. Nowadays, however the need of and hybrid solution IT and TV is probably more realistic than it was tried before. Because of this issues, useability can be seen as an hot topic in e-Health. It is a quality factor which can be characterised with the terms: effectiveness, efficiency and user satisfaction. To measure useability the mentioned terms should be analysed. Once an analysis is done, it is later possible to evaluate and judge in which part of the IT implementation the weakness lie and what can be done for a better solution. Motivation and special training procedures could help to convince the staff about the valuable IT system. In some cases the users may have different opinions about how an IT solutions should be solved, this can result in late projects, lack of acceptance and wrong implementations. From this, it can be concluded, that having people inside steering groups who has knowledge in medical pathways and computer science[8] could benefit the whole project.

To understand how to build user friendly applications, it is important to figure out the need of the user groups. These can be achieved by testing some representative users, and evaluate their behaviour according to their needs and goals. Since a software system nowadays, can be very complex, it might make more sense to test parts of the software system than the whole. Coming back to the main rule, a software solution should be measured during each step of the software project and the stakeholders specially the user group should interact during these processes by exchanging information. This job is normally ensured by the project manager and head of the project. He is the one who can set the goals by using

[8]Or in Medical Informatics.

specific guideines like the ISO 9241, (ISO10a). Nevertheless, the literature give a bunch of inspection methods to assure "user friendliness" like heuristic evaluations or metrics.
Another big issue is the organisational structure and the decision makers behind it. It seems common that for instance inside job descriptions the applicant must only fullfill the knowledge of "Excel and Word" in order to get an IT job in an e-Health branch. But IT is definitely more than that.

## 3.1 e-Health vs. Security

To get an understanding of e-Health and Security the following questioned should be answered in advance before any security policy can describe the concepts further:

1. Do you think that your IT systems are secure against intruders?
2. Would you contract third party consulting companies to check your IT systems?
3. Do you think IT security is an important issue?
4. Is there a mechanism to detect that the system is leaking?
5. What kind of procedures will be proceeds in such a case?
6. When were your IT systems hacked?
7. Do you have problems with viruses, spam etc?
8. Does the organisation have a security architecture?
9. How much does your organisation spend on security?
10. Are you planning to improve your workflow through IT by establishing and linking institutes?
11. Do you have a new procedure which will be introduced soon, for example smart cards?
12. Do you exchange data within other organisations? Hospital → Practitioners?, Hospital (A) Hospital (B)

## 3.2 Security vs. Useability

Security and useability principles are very much dependent on each other. Having a high rate of useability results in low security level. High security on the other hand results in low useability, the challenge is to build systems which can assure both and can bring both terms into balance.

### 3.2.1 Biometrics the missing part

During the last sections the discussion of useability, showed how important this issue is. Can we say that biometrics is the missing part to ensure useability and security, well, biometrics is a form of recognising other people by their shape of face or the sound of a voice. It can be used to automatically characterise a person, according to how their physiology or their behaviour is. Someone may think that this is an area of a new technology developed in recent days, wrong. This technique was used during 2000 BC where ancient babylonian signed with their fingerprints cuneiform tablets[9]. Considering the use of biometrics in security application may look appealing, since to determine a person's identity through a physical object such as smart cards or keys have the problem, that they can be lost or stolen. Determining a person through his unique biometrics seem in form of useability easy for the user and on top also effective. To name a few examples:

- DNA
- Fingerprints
- Iris
- Face geometry

However, not all of them can be used for secure authentication. According to (ABC09) the table gives a comprehensive summary about uniqueness, universality, durability and measurebility of biometrics.

| **Biometrics** | **Unique** | **Universal** | **Durability** | **Measurability** |
|---|---|---|---|---|
| DNA | *High* | *High* | *High* | *Low* |
| Fingerprint | *High* | *Medium* | *High* | *Medium* |
| Signature | *Low* | *Medium* | *Low* | *High* |
| Voice | *Low* | *Medium* | *Low* | *Medium* |
| Retina | *High* | *High* | *Medium* | *Low* |
| Face geometry | *Low* | *High* | *Medium* | *High* |

To be suitable for a security application such biometric data should be

- Unique → not two shape objects should give a access to a system
- Long term use → the shape object used as biometrics should stay constant over time
- Measurable → accessing a system trough biometrics should not cause to much intelligence, hence preferably it should be computable

[9] R. Heindly, System und Praxis der Daktyloskopie, De Gruyter, 1992.

Biometrics solution exists in many areas, like in e-Passports, at the airport, on laptops etc. however, most of them are not appropriate for best security protection. Hence, it is important to analyse the use case, in which area Biometrics could be used. Coming back to the use case of the German Health card, the first and second step which was the authentication step, in this specific case, such an implementation could be usefull. The useability rate would be very high and the authentication procedure would be sufficient too, since the mutual acceptance of the patient and doctor is ensured. They are at the same place and both trust each other.

# 4 Securing the Network

In securing the dataflow the security policy , see figure 9 needs special attention. In most of the e-Health institutions a security policy is not maintained well or it lacks acceptance from the management line. In most cases only the administrator is aware about such a policy but not the head of the organisation. Because of that, the responsibility lie on the IT department itself, without considering the whole organisation as one unit. The key factor in any IT networked environment is, to follow a strict policy plan with evaluation methods, of how the plan is implanted practically. The security policy describes legal and social responsibilities, with objectives of the organisation. A networked system is build up in a complex way, it consists of hardware, software like operating systems, or applications for different group of users. As the institution grows, it is crucial to document objectives, aims and to have a procedure of how to act in case of an attack, like the question, what should be done in case of impersonation of servers through remote access. For each possible attack on the assets of the organisation, there should be guidelines, documented of how a countermeasure could look like. Having a policy encourage user to be aware about security related questions and lower the likelihood of been attacked by social engineering techniques 4.3.

One example of bad efficiency and a doubtfull procedure of transferring data is the case, that in some radiology institutes, x-rays from (PACS) of patients are send by taxi drivers from one location to the next. This shows how conventional methods are still used in a bad inefficient way. Nonetheless, if this procedure is legal should be considered too.

There is no definite solution to protect a system and its data. Regarding the OSI modell, see figure 10 the vulnerability and breach may occur in each of the these layers. The dump rule of protecting the data is, hower, to use encryption as early as possible [10].

In a layered approach , such as the OSI suggest, the interconnection of each layer tend to be the weakest point, from the security point of view.

To protect an institution a firewall may help to secure parts of the institutions assets. A firewall is a collection of countermeasures to secure a network. The firewall divides a network from an unsecured area, like the internet and a secured area. We have different type of firewalls, in which each of them has their pro and cons.

[10] Since applications inside e-Health institution does not consider security issues, they are on the risk.

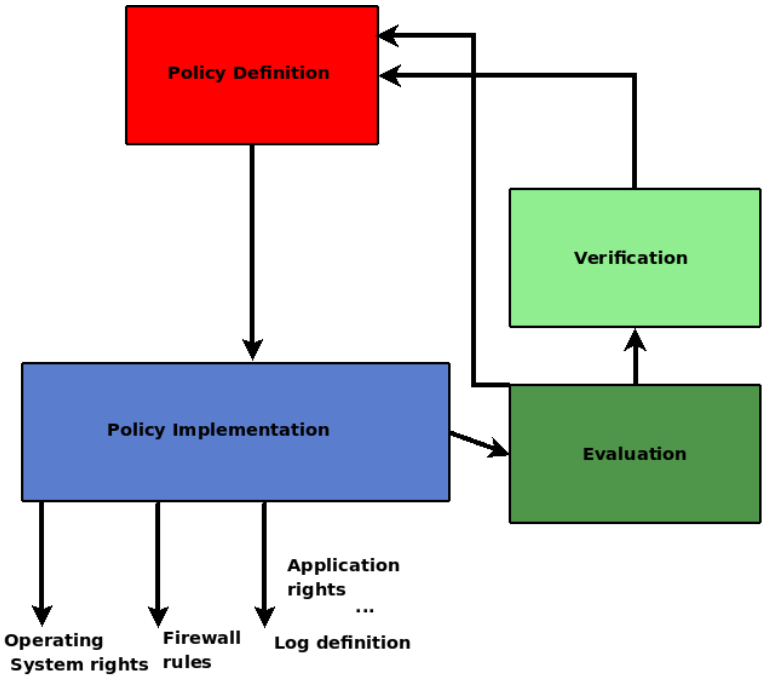



Figure 9: Policy Definition

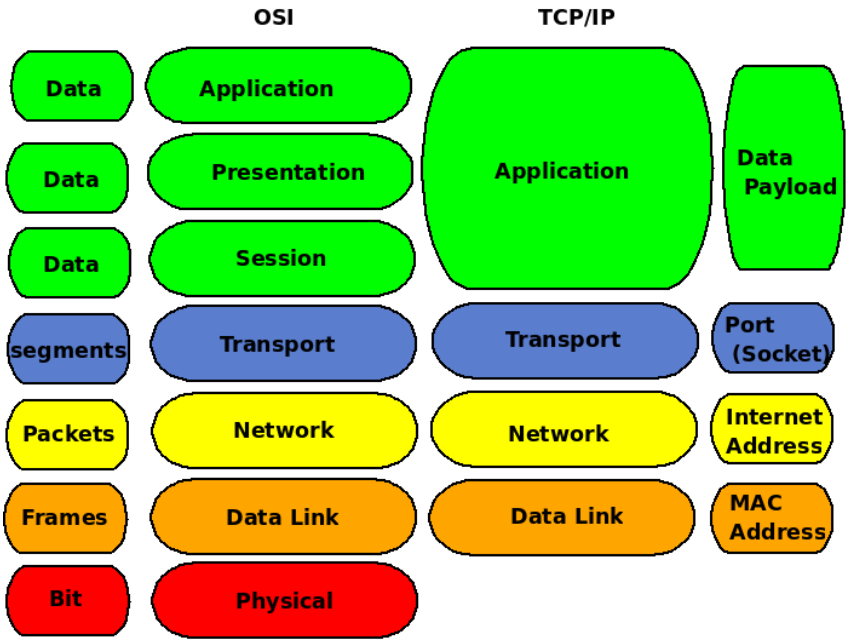



Figure 10: TCP/IP vs. OSI

**Packet Filter**

This type of firewall analyses the communication channel on the network on the transport layer. According to IP-addresses and port numbers of the receiver and sender, the decision is made by restricting or allowing the transfer of the data. In modern implementations the header information of the packets can be analysed. The packet filter solution is easy to implement and to maintain. For the administrator of an e-Health institution, it is easily possible to implement such rules, so that the likelihood of missconfiguration is relatively low. The drawback on the other hand, is obviously, the way it is analysing the incoming packets. It is too simple, since the packet filter is not able to recognise if a communication channel is the channel which it pretends to be, hence no state can be saved. To underline this issue, it is possible to modify a mail server such, that the communication channel is established through TCP port 80, eventhough port 80 is normally used for http connections. This schema is called tunneling and to protect against such tunneling attacks the application gate firewall was introduced.

Stateful Inspection Firewalls

Applications that run on top of TCP follow a typical client/server model. For instance, transmitting email goes from the client system to a server, where the helper protocol SMTP is used. The client generates the email and SMTP uses a TCP connection between the client and server, with this type of Firewall the higher layers, namely the context of the packets are checked before transferring data can be allowed. When a TCP connection is established the TCP server port number is 25. The TCP port number of the client will be chosen between 1024 and 65535 and will last temporarily till the TCP connections ends. A stateful inspection firewall will save all the outbound TCP connections, with other words, for each established connection the entry will be saved inside the firewall machine. Only incoming traffic which are recorded, only those packets are allowed to pass the firewall. Some stateful inspections firewall can save also the sequence numbers of the TCP protocol, this prevent to guess them in order to hack through the system, also called as session hijacking .

## 4.1 Managing IT Security

Managing IT security requires an understanding of the assets each organisation have. According to the assets, also deep understanding of information workflow and the term information security must be considered separately and both in combination. A process, more an iterative process, see figure 11, can be effectively measured through the identification and mitigation of present risk, as well as allow feedback control into the process to mitigate future risk.
In order to manage IT security the management need to have control over their IT security state, as well to be able to act in a time efficient manner. Beside this, specific standards and certification might bring benefits to achieve the goals set. However, it is impossible

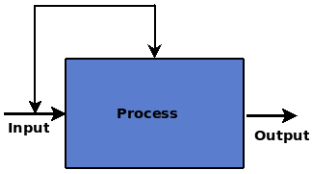



Figure 11: Feed-Forward control

to certify an institution when it has not introduced any security related management processes before. Normally, at least two years should be last, since a certification can be done. Especially, the whole institution must contribute in a way to fullfill the requirements. One important requirement is for instance, that management processes are audited and well documented. The institution would gain the following advantages and these are important in their role towards the huge IT complexity within the e-Health sector.

- Gaining trust towards, patients and practitioners outside the hospital
- It brings control to the security management process
- Benefits towards use of best practices
- Important for marketing argument, since convincing the idea of IT benefits inside e-Health organisation is sometimes impossible
- Cost reduction on the long term
- Further projects success

### 4.1.1 IT Project Management

Project Management abilities are important in any organisation, it can benefit the whole institution when the management knows about the project topic.
A project has a number of specific limited resources, like money, people, and materials. These are used in a way to achieve milestones and to bring the project to a success. The duration of the projects is typically limited by a starting and ending date, also called project closure. Between projects and operations there is a distinct difference, operations are day to day procedures, where a project is mostly unique, individual and last on the specified agreement made within the stakeholders. Introducing software system for a healthcare institution could be one example of a project.
A project has constraints in which the project managers options are restricted these for instance can be:

- Tight deadlines
- Resources

- Government restrictions
- Hardware requirements
- Money
- Reuse of specific interface

or any other limitations. To summarise, starting a project has three universal constraints:

1. Time: The schedule wants that the project is finshed on a fixed date.

2. Cost: The budget is restricted to an amount which should not be exceeded (otherwise project may fail).

3. Scope: The requirements needed to bring the project to closure and the specification of how to achieve it.

### 4.1.2 ITIL

ITIL stands for IT Infrastructure Library and it is known as the standard framework for IT Management, Implementation of IT processes and IT services. ITIL has an huge library of "best practices" which are tested and recommended for organisations of different size. Aims are to specify the needs an organisation may have. Recommendations are given independently from software - hardware vendors and from existing technologies. Its origin has ITIL in Britain, where government agencies recognised the lack of process efficiency within their institutions. The British Central Computer and Telecommunications Agency, short (CCTA), where requested to start building up a documentation schema where "best practices" are documented and standardised, with the objectives to control security, quality and economic efficiency throughout the processes of IT services. Since then, ITIL is well known and more and more institutions from banking sectors to e-Health organisations focus their strategy according to ITIL recommendations.
Organisations are nowadays starting to implement ITIL. They realized that a standardised concept of workflow improvements by using their ressources are needed since:

- Flexibility
  IT systems must be flexible to adapt to different objectives needed, since the customer or government regulations force them to be flexible.

- Uncertainty
  Uncertainties grow with the complexity of systems and technologies used within the organisation

- Customer satisfaction
  Customers, in our case caregivers who have to use systems want quality, efficiency, availability and must be satisfied (useability).

Result and implication of nowadays fast technology changes are:

- Outsourcing
  Low lasting technology duration and the implementation of it makes it hard for organisations to keep and develop that specific knowledge, hence the market for outsourcing grows, hence to keep inhouse knowledge inside organisations is almost impossible.

- Trend Globalization
  Availability of qualified employees in developing countries, makes services to be outsourced, due of economic reasons.

The strength of ITIL is based on following:

- Standardise methods and strong customer focused
- Accepted by many organisations world wide
- Based on "best practises" which can be implemented practically into any organisations, in case requirements are fullfilled
- Can be seen as a first roadmap step to ensure security and quality management
- Good framework for process-oriented-organisation of IT resources

Drawbacks of ITIL are:

- ITIL is on the management layer, especially for the planning phase weak
- Work is focused more on services but less for software engineering projects
- IT procurement is not part of the ITIL catalog
- ITIL is referring to BS7799 Norm and is not considering IT security processes and issues inside its framework
- Training of staff and interchanging of knowledge not given, see "top down approach"

However, chances grow when ITIL is used from an IT security process point of view. Through the introduction of ITIL an institution can gain improvements towards measuring the state of their systems, somehow it can be used like a metric to keep an actual state and improve it through a step by step process.
The following figure 12, according to (BSI09), describes the fundamental parts of ITIL. IT consists of specific key publications, each of them are connected to each other. Five of the seven publication handle the IT Management areas such as:


Figure 12: ITIL components, (BSI09)

- Service Management
- Application Management
- ICT Infrastructure Management
- Security Management
- Planning to implement Service-Management

The other two focuses on Service Delivery and Service Support.
To sump up ITIL shows how IT process Management between clients or from the business point of view can be connected within existing technology. The foundation which can be seen as a bridge can be build with the areas mentioned above.
From the Business perspective ITIL describes the following aspects:

- Changemanagement
- Partnership and Outsourcing
- Quality Management
- Customer Relation Management
- Planning and Control Management of IT Services
- Business Continuity Management
- Business and Management Knowledge
- Propose IT Organisation

Service delivery brings the idea of how specific tasks can be efficiently delivered to the customers. It focuses on process service management, like planning, documentations, and optimisation of IT services[11], where the following areas describe the processes involved in service delivery.

- IT Service Continuity Management
- Capacity Management
- Financial Management for IT-Services
- Service Level Management
- Availability Management

Service support regulates the operative tasks of the service management procedures. To ensure service quality, ITIL recommend to compress different application interfaces into one and divide services into the following five units.

- Service Desk Function
  Handles customer support and it is the main interface to the customer.
- Problem Management
  Ensures to recognise failure inside IT infrastructure and to develop countermeasures to resist against repeated hacks.
- Incident Management
  In case of incidents, the institutions should have a plan B where it must be possible to react in a short period of time and to make the agreed service available.
- Change Management
  Ensures to use standardised methods, to change desired services in a short, efficient, and without big impacts for the users.
- Release Management
  Release Management ensures to roll out only tested software and hardware versions.
- Configuration Management
  Ensures to verify the status of all IT equipment used and the relationship between each other. IT makes sure to document unique data of processes needed.

[11] Any incident like power loss.

### 4.1.3 ISO 27001

Beside ITIL, which brings the discussed benefits, the standard does not consider IT security at all. Because of that there is a structure needed, which manage these important security management issues. One of the most important standards related to security is the ISO 27001 standard.
The consits of the following modules.

- Business Continuity Planning
  Mainly it defines critical business processes.
- Access Control
  Control access information
- System Acquisition, Development and Maintenance
  This involves securing the infrastructure, the application software and to protect and ensure CIA.
- Physical and Environmental Security
  Padlock etc.
- Compliance
  Aim is to maximise effort on effectiveness, minimise inference to/from the system.
- Human Resource Security
  Main task is to reduce the risks of human error, by training users to be aware of information security threats. Important is hereby the factor of happened incidents, it should be ensured that lessons are learned from incidents occurred in the past.
- Organisational Security
  Manage and maintain everything about information security within the organisation by internal staff or by third parties (outsourcing).
- Computer and Network Management
  Ensures availability in term of system failure and the reduction of it. It tackles software damage, loss, modification or misuse and it protects the integrity of the information exchanged between organisations.
- Asset Classification and Control
  Equipments are tagged, in our case medical equipments according to its value, with other words appropriate level of protection is assured to the assets.
- Security Policy
  It provides a security map of how a path and support of information security can be given.

- Security Incident Management
  This module simulates incidents and anticipate them to a specific level. It must be assured that the management can cope with an appropriate response to security breaches.

- Risk Analysis
  Risks which may occur, for instance measuring with the help of Program Evaluation Review Technique (PERT).

The figure in 13 gives an informal insight about the certification procedure.

- During the pre-checkup or pre-assessment fundamental security risks are identified and need to be resolved before the certification-assessment can be positive. The result of the this phase is well documented and according to the risks found classified.

- During the second phase the main certification procedure starts where all relevant units must have a security management concept. When failure are found, then those need to be eliminated and a re-assessment must be proceed.

- In case the assessment process was positive the result will be send well documented to a certification authority, where the formal certification is accredited.

- The last phase of the process makes sure that the certification is up to date and this check up is done annually.

Once the certification is applied to an institution, it is approved to state this for three years. Implementing new technologies or fundamental changes after the certification must be announced so that appropriate actions can be taken.
To sump it up, the standard itself is not a complete dictionary of how to face vulnerabilities and its countermeasures, it is more a systematic way to bring control inside institutions where IT security plays and important role. Risks are evaluated and it is assured to handle CIA. Like the ISO 9000 standard these check ups are done through the Information Security Management System (ISMS), where risk management, security policy, legal requirements, authentication control, system development and maintenance inside the organisation are controlled. The standard is internationally known and practically tested as well.
How could a framework for the e-Health branch looks like? If we consider the branch as a black box what kind of "security" can we proclaim is best? These questions can not be answered at this moment, unless there is a definite security policy which sets the expectations wanted.

## 4.2 Top down approach

More and less most of the e-Health institutions have almost the same problems introduced in section 2.1. During this section, the idea is to introduce a solution of how e-Health institution can challenge with the problems they face today. The problems discussed

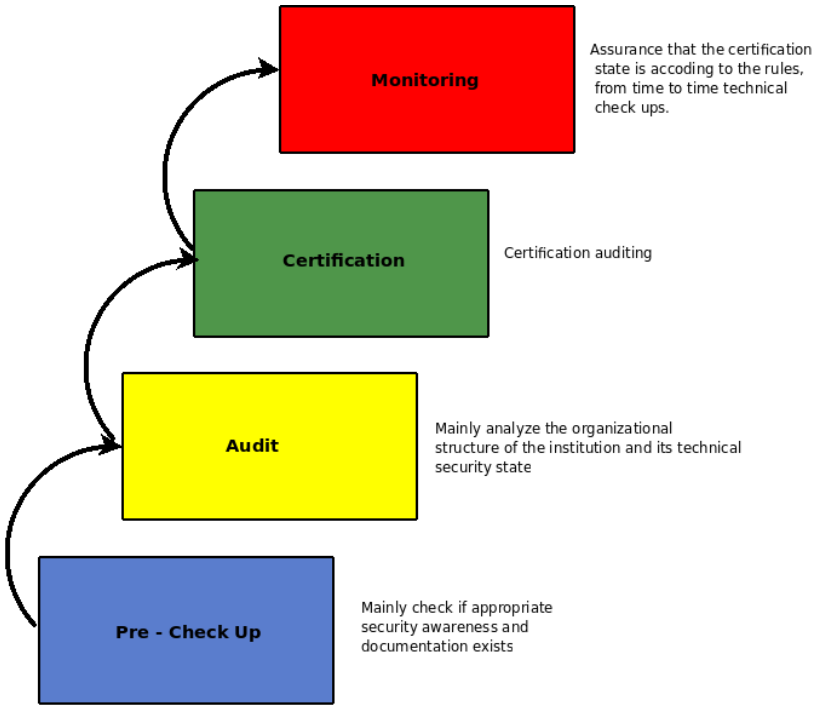



Figure 13: ISO 27001 informal certification procedure

during the last sections can be solved by a mechanism from top management to employees and resources up to stakeholders within the organisation.
According to my findings and the scientific surveys, the top down approach would benefit any e-Health organisation, which lacks process control, lack of communication within the organisation and more important, lack of awareness about security related questions. This top down approach purpose is a way to bring structure into the e-Health institutions. From the top management to the stakeholders involved within the institution a transfer of needs and knowledge can be undertaken. If we consider, that we can simplify an e-Health organisation like an hospital, as an example according to the figure in 14, we can assure knowledge management through:

- The Management
  Typically the management inside an hospital environment is lead by a combination of medical doctors, from the field of medical informatics, or by medical doctors with an educational background in economics. The drawback is that there should be a team of all these disciplines, with other words the field of computer science, economics and medical knowledge should be part of the institution. In most cases one or more backgrounds are missing.

- IT
  The IT department consist by individuals from different backgrounds, since the fact

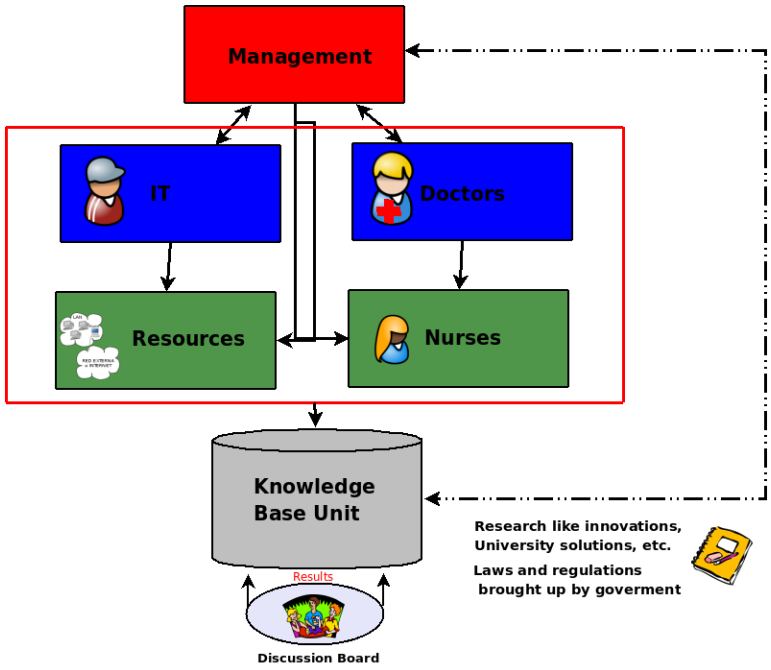



Figure 14: Top Down Approach

that someone could study informatics only from 1970s, and that knowledge, hardware, software changed rapidly we can draw the conclusion, that most of the employees[12] are not up to date within the field of computer science / IT security.

- Resources
  IT resources such as software and hardware solution are bought from different companies who has their best and cons, however the problem lies, that different solutions are integrated together, which results in island solutions in addition, which are on top also incompatible with each other.

- Doctors & Nurses
  It is crucial to understand the needs of the staff, in this case doctors, nurses and other relevant employees, whose job is to treat patients and has responsibility over the care unit. From the IT perspective, it must be assured, that the IT systems they are using, are made to work efficient and the data presented is reliable. A relationship of trust should exist between the entities user and the IT systems maintained by the IT department.

- A knowledge based transfer unit
  A knowledge base transfer unit can improve the communication within the organisation itself. It should be possible for employees to develop and bring up ideas to

[12] Especially civil servant.

a discussion board. This can be achieved through a knowledge based transfer unit, which main tasks is to transfer knowledge within the organisation. How a transfer unit is constructed depends on the organisation itself. It can be a software solution, could take place in form of meetings, or for instance, as an e-lecture portal within the intern network of the institution. If this is the case, a voting mechanisms should be part of the solution, so that employees who introduce ideas can get a feedback from the whole staff including the management. Positive ideas brought up by an employee should be encouraged and should result in benefits [13]. One positive aspect would be communication improvements between the staff and the management can adjust the need of the organisation according to the present circumstances. Once such a system is introduced, the awareness of IT security topics within the staff can be introduced systematically. A top down approach also helps to identify weak or critical parts of the institution. It brings a first step procedure, to have a plan for incidents or a structure of how to move on to an efficient workflow environment inside the organisation.

Last but not least, such a unit could motivate the staff to bring new ideas which may be introduced into the institution, and which can benefits the whole organisations.

For most of the employees it is crucial when they get the feeling that someone else is not listening to them or their opinion does not value. Nowadays employees need to know what is going on in their organisation. This is one reason why communication becomes important.

- Discussion board
  Within the discussion board, a compliance about ideas brought up by employees can be achieved. Also voting results would bring topics up to the mind of the stakeholders.

- Result
  Results would be better process workflow, understanding of the needs of e-Health organisations. Procedures needed to undertake and last but not least security awareness.

## 4.3 Testing

A strategy to test IT systems is often called as penetration testing, ethical hacking, or also as tiger team analysis. The penetration test is defined as a wide security test, accomplished bye experienced security professionals, who simulate the behaviour of an real intruder, namely the black hat hacker himself. Penetration testing measures the security level of one system or a whole network of different size. Systems which are connected to public networks, in order, to exchange data over an insecure medium, like the internet, can be compromised. For instance, unauthorised access of confidential data, such as electronic health records, EHR. Numerous risks exists for institutions linked to the public network,

[13] This is up to the institution a benefit could be more money for the same work or a voucher.

where various attacks on vulnerabilities may be possible to gain access to confidential data. The motivation of an attacker could have different origins, from organised e-Crime to self impression and peer recognition to searching for new challenges, many reasons exist. To mention a few reasons which affects the e-Health branch is listed below.

- e-Health institutions are not spending money on security, hence their IT network is insecure, this invites potential intruders.
- What ever we have experienced in other branches like e-Banking, it might affect e-Health too.
- New challenges, are sought by hackers, since criminal prosecution is rare.
- Having accessed EHRs, it can be sold to insurance companies, which for instance can deny membership to people who are chronically ill.
- Hacking, Worms etc. is a money making possibility, we have to face such problems and need to be prepared.

During this testing approach the objective is, to meet the expectations of the client, which must be defined clearly before a test can begin. This is mostly agreed in form of a contract, with obligations on both sides, namely on the clients and testers side. The client must cooperate as much as possible, and provide information, which is needed to penetrate the test. For example, if a white box test approach structure, see figure 15 is chosen, then IP addresses, security policies, system configurations, firewall rules etc. must be handed in to the penetration tester.

The black box approach on the other hand, gives no prior information about systems used inside the network or any other form of information. It is the penetration testers own duty to start collecting information from the scratch, such as IP addresses, DNS servers etc. A combination of black box and of white box testing is called, grey box testing, where some kind of information such as source is handed in to the penetration tester, see figure 15.

During a penetration test, different kind of unforeseeable system failure may occur, so to err on the side of caution, high risky and important systems need to have a backup system, so that in case of failure, the data lost can be restored. Another important point is, that during a test third parties could be affected, also this should be part of the contract, hence the effect is important for the outcome. In the clients interests, the tester must sign the obligation that secrecy is ensured, since a penetration tester may gain access to sensitive data. Information which need to be confidential must be kept confidential. All vulnerabilities found must be well documented and scope of the documentation, the testing procedures and results must be specified in the contract. Hence, a penetration test can be very specific, it may take several weeks. To avoid dissapointments, the starting time of the penetration test and the finishing time, in respect of the stakeholders, must be hold, preferably inside the agreed contract. Shortly said, the purpose of a penetrations test is, to

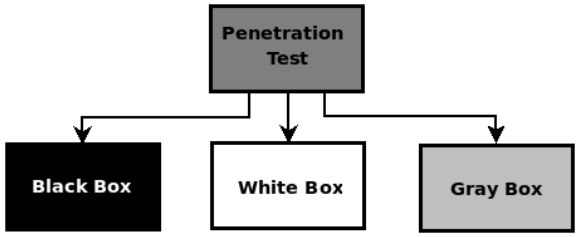



Figure 15: Penetration Testing

ensure and measure information security which is defined as, protecting information and informations systems from unauthorised access, use, modification, and disruption. Hereby the term CIA, known as Confidentiality, Integrity, and Availability, is often taken to define the needs of information security.

- Confidentiality
  Information should be only available to a set of predefined individuals, including assurance of not authorised transmission and usage.

- Integrity
  Data send through a channel should not be altered in ways of modification, incorrect or incomplete.

- Availability
  Assurance that information should be accessible to the set of authorised individuals, by any time, without time restrictions. It is formally agreed in Service Level Agreements (SLAs) used by service providers and their enterprise clients.

### 4.3.1 Penetration Testing

In this section the aim is to give an overview of how the procedures are linked with each other. A penetration tester, simulates a motivated attack for a specific amount of time, to give a snapshot of the current security of a system or a business process. Penetration testing has a few standardised methods like, Pete Herzogs's "Open Source Security Testing Methodology Manual", short OSSTM (fSI09). It is a very practical approach with checklists of what should be tested and in which specific order. A OSI standard, under the number of ISO 27001 , prior ISO 17799 / BS 7799 focuses more on the policy and theoretical part. It is an huge catalog of security controls which defines further a standard for audits. Auditing, on the other hand, analyses for instance configuration files, or for instance source code conformance. Employing testing can be done on workstations and

servers, like web servers, database servers, on infrastructures, like VPNs, networks devices, firewalls or wireless networks. Also the possibility to test the strength of applications can be tested.

Threats can come from two different type of attackers, from outside, like the internet or from from inside, like extranet. Ethical training is the first step when people start working for a new company. Mostly, ethical behaviour is part of the contract, which the employee need to accept before starting the work for the company. However, there are some who do not play by the rule, these are those who are in the IT world called "black hats". They are those who attempt an unauthorised penetration attacks against a system or network. Sometimes these Black Hackers come from different countries where such an attempt is not a crime in their laws, which makes it much harder to bring them to justice. They mostly use different zombies from different locations to gain financial benefits or just to bring the system down, for any other different reasons. However, it seems difficult to draw the line of a criminal act and the fact that an intrusion might help companies. The case of Michael Lynn could be seen as an example [14].
In performing an attack, it is very important that the real attack is simulated. A few examples of who these attacker could be.

**Outside Attackers**

- Competitors
- Script Kiddies
- Terrorists

**Insiders**

- Employees
- Contractors

The penetration test can be divided mainly into two parts, one which involves tools to perform an automated testing, and second manuel testing.
Automated testing can be done, for instance with nmap[15], to reveal open ports.
Here a few examples of an automatic testing.

**Automated Testing**

- FTP source port scanning
- UDP port scans

[14] See more on http://en.wikipedia.org/wiki/Michael_Lynn
[15] www.nmap.org

- OS fingerprinting

During the manual testing the creativeness of the penetration tester is important, for instance, he needs wide fundamental knowledge in SQL and programming experience, and should bring expertise in searching for input validation vulnerabilities, like SQL injection attacks(KS03). Here a few examples:

**Manual Testing**

- HTML injection attacks
- SQL injection tests
- Encryption strength and scope
- Session tracking
- SMTP specific testing, like social engineering, spoofing email addresses

Before stating the objectives, the critical question is who is going to perform the penetration testing, must be answered. Following opportunities exists:

- Hardware supplier
- Inhouse security team
- An individual hacker
- Third party

Against the hardware supplier speaks the fact, that they are to familiar with their product and may be less constructive when testing. Hiring an individual hacker may have the problem, that secrets revealed during the test, are not safe with him. On the other hand, having an experienced inhouse security team, who have deep knowledge in testing, could be the right choice. However, also they could be too familiar to perform the test. A third party consulting company may be the best option. There is no rule of thumb choosing the right tester, but a potential employers of security tester should consider that he brings the following requirements.

### 4.3.2 Requirements

A security tester must bring depth understanding in IT systems, in-depth knowledge of TCP/IP and other networking protocols, OS (Windows, UNIX, Mac OS,) and hardware expertise. Also important is, the attention to record and maintain the ethics of security. A security tester must be at least educated to system administrator level, in order to do his job effectively. As a paid security tester, it is expected to understand what you are doing and all the potential effects your actions may have. Specifically, to understand

the chosen tools for testing, and why the set of tools where chosen, since some of these security tools can cause damage, or result in network failure, if it is not used properly. After the rest a security tester should be able to articulate the methods used, to penetrate the systems and to expose counter measure, of how to fix the security vulnerabilities identified during testing procedure. The knowledge of a tester must be wide in terms of new technologies, such as firewalls[16], intrusion detection systems, sniffer, auditing tools, and of course authentications methods and cryptographic protocols, to mention a few. For each of these their strengths, weaknesses and the products that implement the technology in order to find ways, should be known. Educated in application programming can also be helpful since many new exploits, such as buffer overflows may occur nowadays.

### 4.3.3 Objectives

The value of a penetration test is very much dependend, on the objectives made by the client during the planning phase. Also, the ability of the stakeholders involved is a parameter. Goals must be set clear, in case that they are not reachable, the tester should notify the client as soon as possible. In a nutshell the objectives are:

- **Identifying vulnerabilities**
  Only through the identification of vulnerabilities, the overall security can be improved, hence a security test shows where the problems lie.

- **IT Security confirmation**
  Nowadays, more and more organisations are certified, that there IT systems are tested and that they fulfil a standard, such as mentioned before the ISO 27001 standard. However, only the present situation at a particular point is measureable. The statement made is not valid for the future, hence the fact that a penetration test does not guarantee 100 percent security, it only increases the level of security in IT systems.

- **Improving security state of IT systems**
  For an example, the wireless LAN network of the company can be tested explicitly, to see if it is possible to penetrate from the outside of the network. Another aims could be to determine how vulnerable the systems are from an inside attack.

- **Improving security within organisation, like general security awareness to employees**
  Probably the most important point is that a penetration test might bring general awareness to employees, such that social engineering techniques are detected before

[16] Hardware firewalls.

an attack can be accomplished.

The figure 16 shows what is needed to increase security within an organisation. The

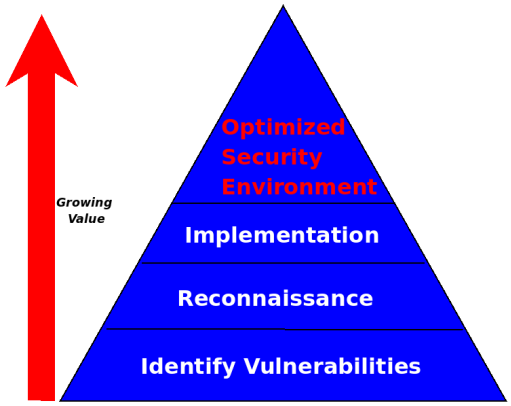



Figure 16: Penetration Testing Value

test itself can be done with different level of aggressiveness. According to (fSI09), the aggressiveness is divided in

- passively
  As the name suggest, it is the lowest level of aggressiveness, where just sniffing tools are used, without exploding vulnerabilitis, which were found during the security test.
- aggressive
  It represents the highest level of aggressiveness, where each vulnerabilities found during the inspection is exploited. Even denial of service attacks (DOS) are performed to completely bring down the system or the network.

### 4.3.4 Planning

Planning a penetration test belongs probably to one of the most important steps. It is the part, in which appropriate inputs needed to be defined, such as existing mythologies, security policies, laws and regulations and last but not least, best practices. Without any doubt, the planning process has an huge impact to the result of the penetration test. This phase of the overall process, makes sure, that the details of starting and ending of the penetration test, the aims set by the client and of how the preparation and the clients expectations are fulfilled. Previous security tests can help planning to set the scope of future tests, for example the question of which strategy, the black box or white box strategy should be chosen.

### 4.3.5 Reconnaissance

During the reconnaissance the search focus on freely available information, which can be used to assist the attack. Pinging the network can be done, to see what IP addresses exist on the network, or looking in forums, where misguided employees of the target organisation left important information. One of the reconnaissance techniques is called social engineering, which is the oldest and still the most effective method of propagating malware and harming networks.

#### Social Engineering

Collecting information as form of a social engineering technique, where collecting information is obtained either knowingly or unknowingly. The minimum requirement for starting social engineering, is the name of the institution or the company. The results should bring:

- Identification of departments inside the institution.
- List of employees who works in the department which is highly important from the attackers side.
- Names, email addresses of candidates for a potential target.
- Organisational structure of the target, hierarchy and management positions etc.

Steps of how to achieve the expected results:

- Website of target organisation and essential information (names, email addresses)
  → effort is low
- Information which are public on news or databases (vulnerabilities found before, branches worldwide)
  → effort is very high
- Search forums for misguided employees through the email addresses, names
  → effort is medium

Different steps may be used, like tapping phones and networks, lying to employees or stealing equipments. In detail the following example methods can be used to succeed during the reconnaissance phase.

- **Search engines**
  Google as a search engine, can be used to find useful information about the organisation, its structure, their employees and confidential data, which were put accidentally online, especially if the search is focused on cached pages. The search query ” unable

to jump to row on mysql result index on line“ for instance can reveal SQL injection vulnerabilities. To perform automatic engine searches, one can combine different search engines and databases, more in (Mid10). Searching for source code, in different forums, may be another option to gain knowledge about ownership, developers name etc.

- **Social Networks**
  Having a name or email address can be used to collect more information about employees, like home town, pictures and so on. Since social networks are mainly interested in connecting as many users as possible, they make sure, that their users are easily findable, with other words their search engines are very efficient. There are tools which helps to find email addresses and which can be combined with search engines, in a way that a specific site for example, *www.for-instance.com* can be taken as a starting point. Once the tool is used the outcome will reveal email addresses which belongs to the page *www.for-instance.com*.

- **CVs**
  CVs can reveal many important sensitive information, like projects and specific systems the employee worked within the company, for instance SAP, MySQL, Oracle, Unix, etc. With this kind of information the attack can be done more specific, since the attacker can try to build up the potential network and gain an idea of how the infrastructure might look like. It seems very much common, especially in UK, that CVs are requested in *.doc format. Once uploaded to the recruitment agencies, the data may be read out. This does not mean that only *.doc formats are a threat, also PDF, etc. could be a target, only that the *.doc, txt etc. versions may be more easy to read out than *.pdf versions. From an malicious attackers points of view, it seems it might be worth searching for vulnerabilities inside work agencies network. In job postings, the same procedure can be used, to try to find useful information. Mostly, when posted also the email addresses of the hiring manager is included. An email address gives always a good starting point for more research.

**Technical Reconnaissance**
Under technical reconnaissance we understand the use of the target system which we use to gather information.

- **ICMP**
  Ping is a program which produces ICMP messages to the receiving system, once a request is send the reply message is send back to the requesting system. Sending an ICMP message and receiving an answer shows, that the host is alive and available for an attack. However, this ICMP request were used in the past to attack targets with Denial of Service (DoS) attacks. Many organisations, hence do not allow ping requests.

### 4.3.6 Enumerations

During enumeration phase , the focus lie on network vulnerability discovery. Without setting fixed expectations during this phase, an overview of the target environment is build. To accomplish this, many helper tools may be used. The following figure 17, shows the steps in information gathering, according to (Gra07). Hereby, footprinting is a technique to gather information by using specific tools, to discover operating systems run on the target system or other useful information. The aim is to get a greater view of the network.

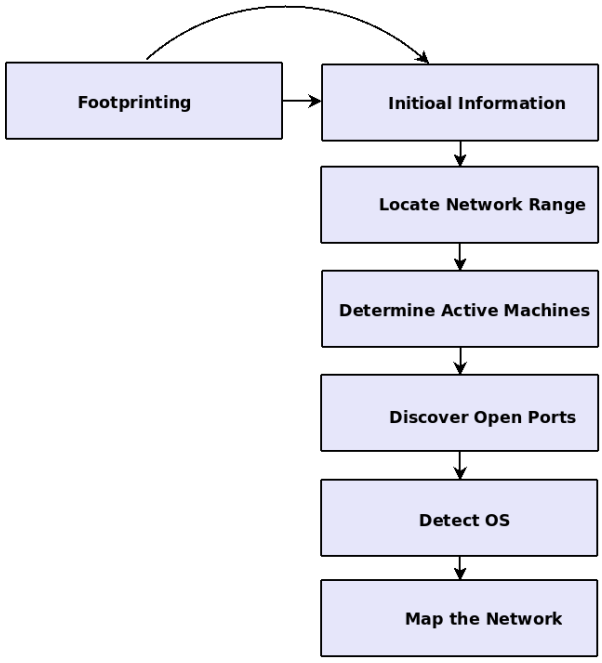



Figure 17: Six steps of Information gathering

Nmap is probably the most well known valuable port scanning tool. A port scan, uses the typical communication setup between two entities by manipulating it. With other words, the port scan provide information, of which ports are open or closed. With these information, a detailed attack plan can be build. It is a tool to conduct a networks survey and it is suited for scanning large networks. Furthermore, it can determine what operating systems are running on a network, as well as the type of packet filters and which kind of firewalls are in use. The figure 18 shows a typical run of nmap, with explanation.

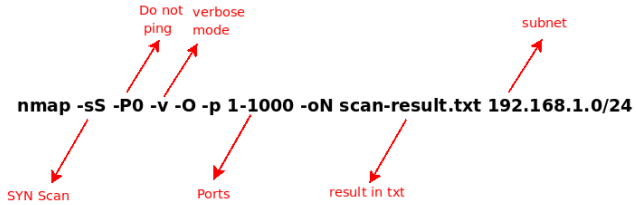



Figure 18: Typical nmap SYN scan

**Scanning**
We can distinguish three types of scanning, namely:

- Port scanning: Search for open ports and Services
- Network scanning: IP Addresses
- Vulnerability scanning: Present and know weaknesses

There are many different techniques, which can be used to succeed during the enumeration phase. As we know the internet is based on the TCP/IP protocol. TCP is a connection oriented protocol, which is used by systems to interact with ports. SYN scanning 18, FIN scanning, fragment scanning and many more are types of how to use the TCP protocol to start a request, and according to the scanning technique, reveal information about the target systems. But it is of course possible to use different other protocols like FTP, UDP no mention some. These techniques are mainly focused on how to investigate the targets technical systems, which are in use, what type of application exists, and generally to get as much information as possible about the environment of the target organisation. The next sections explain some of the enumeration techniques, which can be used.

**SNMP Enumeration**
SNMP enumeration is a process to enumerate user accounts of a target system. Simple Network Management Protocol (SNMP) is used mostly in systems, where the devices attached are monitored. All network devices, such as routers, switches etc. contain an SNMP agent which is used to manage the devices. The SNMP station sends requests to the agent, in which the agent is responsible for the answers. On the networking device, the Management Information Base (MIB), is in charge of a database, which is managed by the management station. The management station can for instance change, the variables

which resides in the database through a request. There are two passwords, one is needed to access the SNMP agent from the management station, one is used to change or edit the configuration on the device. In case of missmanagement the passwords can be left at the default settings, a lookup at www.defaultpassword.com, a hacker can use default passwords to view or change the configuration of the device.

**Stealthy Port Scan**
The stealthy port scan identifies which services each device is offering, with which operating system.

- Expected results
  Which services are offered by the device.
  Identification of the operating system.

- Test steps
  Perform a port scan which is from the target side undetectable or difficult. This can be achieved by using specific parameters, when tools are used. A good method is to delay the scanning by some intervals.

- Risks
  However as stated above, it might be possible that the scanning is detected.

Scanning assumes that the interactions to the systems are identified, like for instance IP numbers which are accepting connections, are known. The purpose is to find out which services are in use, specially which open ports exists. Nevertheless, the versions of each protocols in use is also a good starting point. Consider the following example: #telnet www.example.com 80
#HEAD / http / 1.5
#[cr]
#[cr]

This will reveal the information of which web server on the page www.example.com is used.
#HTTP/1.5 200 OK
#Date: Tue, 2 Mar 2010 23:03:09 GMT
#Server: Apache/2.2.15 (Unix)
#Last-Modified: Wed, 11 Sep 2010 15:20:21 GMT

Below some additional tools which can be used to perform scanning:

- Hping2 (powerful Unix tool, to gain important information about a network)
- Netcat (also known as the "Swiss Army knife" of network utilities)

- Traceroute (shows the hops of the network and the route to the target system)

Scanning can disrupt network operations by consuming bandwidth and slowing down the network response times. However, a network scan opens an organisation the opportunity to maintain control of its IP address space. It can also ensure that its hosts are configured according to their agenda, to run only approved network services. To minimise the risk of disruptions within a network, the scanning software should be carefully selected. When a network scanning is done, it results should be well documented.

### 4.3.7 Vulnerability Analysis

During the last steps, reconnaissance and enumeration, we tried to get a better view of the target systems and we collected, the information we could and now during the the vulnerability analysis phase, we practically try to match found vulnerabilities with known vulnerabilities. Known vulnerabilities can be found on different pages, like for instance, ISS X-Force[17] or under Exploit World [18]. By doing this, the penetration tester will try to identify hosts within the target network, with all open ports and the operating systems, as well as running applications. This includes the patch level of the OS or service pack applied. To manually match these, the penetration tester should have a collection of exploits available, to determine which exploit may be possible on the target systems. There are a few tools available which automatically can detect vulnerabilities. Such a tool is for example Nessus[19]. Nessus is a security scanner, which remotely ensures if a given network has vulnerabilities or not[20]. Once information is collected, each vulnerability need to be analysed in a way so, that each possibility is weighed, according to the plan, which was agreed during the planning phase. During this investigation, it must be asssured, that the vulnerability found is practically exploitable against the target system. To minimise the risk of harming the target, it might be possible to stop penetration testing at this point, and fix those vulnerabilities found. The target can get recommendation in a form of a sheet wit a step by step procedure of how to eliminate the vulnerabilities.

### 4.3.8 Exploitation

Exploitation is also called penetration attempt which can be divided into a five-step procedure, see figure 19. Each step formulates important processes during an exploitation. For instance, if a password cracker is used to determine the password of a SNMP system, one can use appropriate dictionaries and tools to succeed. This involves mainly the steps, gathering information, testing and planning the attack, according to the figure in 19. After gaining a users password, rootkits can be installed to get something like an "all access card". Once the rootkit is installed, the hacker can come back to the system at a later time. Rootkits represents an highly threat to the system, once it is compromised.

[17] More info under http://www.iss.net/security_center/
[18] http://www.insecure.com/sploits.html
[19] http://www.nessus.org.
[20] Of course this does not guarantee, that there are no other security flaws.

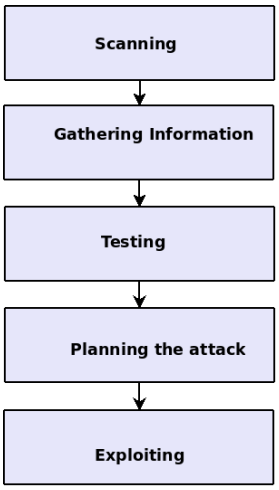



Figure 19: Five-Step Attack Procedure

### 4.3.9 Conclusion

It is difficult to define the threats in information systems and thus harder to know in which direction it is going. Because of the threats we are facing today, it is important to regularly check IT infrastructures of an organisation. Especially from the application point of view, where the threats are rising, there is a need of a security testing procedure, called penetration testing, which measures the actual level of security. Penetration testing helps the organisations make their employees aware of security. It ensures and train employees to understand typical social engineering techniques and train employees, who are the weakeast link in the chain. Education in IT security brings many advantages to the organisation and the employees itself. Hiring penetration testers keep the level of confidentiality, integrity and availability high, even though the limitations are, that 100 percent security of the IT systems can not be assured. One of the most important benefit is, the fact, that the test is not just about reporting problems, also it makes sure to provide recommendation in the most efficient way of how to secure and fix those vulnerabilities found.

# 5 Conclusion

The thesis objectives were to introduce the topic of IT issues and solutions under consideration of the fixed requirements e-Health institutions have. These were to consider their specific protocols, their specific approach towards new implementation solutions and the importance of regulations. After discussing the actual state, the issue of a systematic top down approach was given, which handled the gap of the mentioned IT management procedures of ISO 27001 and ITIL. Hereyby, recommendations were given to use ITIL as a starting point and carry on to the certification process of ISO 27001, which handels security concepts of an organisation. The top down approach was introduced to benefit the

communcation structure within the organisations itself, since promoting security requires that particapants and users need to be aware of fundamental security risks occur, especially then when regarding the high vulnerabilities rise of applications. It is also important to look at the needs

# References

[ABC09] C.A. Ardagna, C. Braghin, and M. Cremonini. Net privacy. In J.R. Vacca, editor, *Computer And Information Security Handbook*. Morgan Kaufmann, 2009.

[Atk98] Randall Atkinson. Security architecture for the internet protocol. Technical report, 1998.

[BBC09] BBC. New 'superbug' found in uk hospitals. http://www.bbc.co.uk/news/health-10925411, August 2009.

[Bel89] S. M. Bellovin. Security problems in the tcp/ip protocol suite, 1989.

[BSI09] BSI. Itil. BSI PRESS, August 2009.

[BSI10] BSI. Durchfuehrungskonzept von penetrationtests. BSI PRESS, March 2010.

[Cis10] Cisco. Cisco Security Advisory: Cisco IOS Malformed OSPF Packet Causes Reload , 2010.

[Eys09] Eysenbach. e-healh. http://www.jmir.org/2001/2/e20/, April 2009.

[fSI09] Institute for Security and Open Methodologies (ISECOM). Open source security testing methodology manual. http://www.isecom.org/certification/owse.shtml, August 2009.

[Gra07] Kimberly Graves. *CEH: Official Certified Ethical Hacker Review Guide*. SYBEX Inc., Alameda, CA, USA, 2007.

[Gua09] Your Local Guardian. St helier hospital power cut affects special care baby unit. http://www.yourlocalguardian.co.uk/news/4671431.Hospital_power_cut_affects_special_care_baby_unit, October 2009.

[Hos09] Hospital. Warning fake employment offer. http://www.klinikum-nuernberg.de/DE/aktuelles/neuigkeiten/warning_fake_employment_offer.html , August 2009.

[II10] Inside-IT. Gefaehrliche pdfluecke entdeckt. http://www.inside-it.ch/, September 2010.

[ISO10a] ISO. Iso 9241. , March 2010.

[ISO10b] ISO. Iso27001. www.17799central.com/iso17799.htm, March 2010.

[Jee09] Jeek. epassports broken. http://freeworld.thc.org/thc-epassport/, October 2009.

[KS03] Amit Klein and Director Of Security. Sql injection. Technical report, http://www.packetstormsecurity.org/papers/bypass/\Blind_XPath_Injection_20040518.pdf, 2003.

[LK73] Shen Lin and Brian W. Kernighan. An effective heuristic algorithm for the travelling-salesman problem. *Operations Research*, 21:498–516, 1973.

[Lou99] Francisco Louca. Nikolai Kondratiev and the Early Consensus and Dissensions about History and Statistics. *History of Political Economy*, 31(1):169–205, 1999.

[Mid10] Midnightresearch. Search engine assessment tool. www.midnightresearch.com/search-engine-assessment-tool, March 2010.

[Mil09] Elinor Mills. Conficker infected critical hospital equipment, expert says. http://news.cnet.com/8301-1009_3-10226448-83.html, April 2009.

[Org10] IHTDSDO Organization. IHTSDO, 2010.

[Oys10] Oyster. Oyster public transportation. http://en.wikipedia.org/wiki/Oyster_card, October 2010.

[Pre09] Associated Press. It was the '60s, man. http://www.wired.com/science/discoveries/news/2005/04/67254, April 2009.

[SAN09] SANS. The top cyber security risks. http://www.sans.org/top-cyber-security-risks/?ref=top20, April 2009.

[SKK+97] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. Analysis of a denial of service attack on tcp. In *IEEE Symposium on Security and Privacy*, 1997.

[SNO10] SNOMED. SNOMED CT, 2010.

[the09] theHarvester. Technical report, http://www.edge-security.com/theHarvester.php, 2009.

[vW10] Kenneth R. van Wyk. Penetration testing tools. https://buildsecurityin.us-cert.gov/bsi/articles/tools/penetration/657-BSI.html, March 2010.

[WT04] Brigl B. Winter A. Wendt T., Haber A. Modeling hospital information systems (part 2): Using the 3gm2 tool for modeling patient record management, 2004.

[Zia07] Najib Ziaie. Computer Science Methods for the Optimisation of Workflow in Hospitals , 2007.

# Index