Seminar session 2

Threat modeling and cyber security design approaches using the example of Scotland's Health System.

Background to the problem:

- Scotland's Health System (on the Web)
- NHS Scotland Health includes 14 Boards
- One of it is called "Fife"
- Offers many differnt health services (e.g. Neurology, Psychology, Radiology,...)

In the following, the Radiology service is taken as an example.

An important feature for radiology is the PACS system.

PACS System: Picture Archiving Communications System

- Access to Radiology service is through a referral system.
- Radiology examinations are stored and reported digitally.
- Imaging is accessed by a Consultant Radiologist and compiles a report.
- Report is sent to the health professional that made the request.
- PACS is a national system – accessible across all health boards.
- Accessible by both Radiology staff and clinicians.
- You must be a doctor or be highly specialized in your clinical field to be able to read x-rays and act upon them.
- Integrates with Image Exchange Portal (IEP) for safe and secure transfer of imaging to specialized healthcare institutions around the UK.

A digital System must achieve the design obectives: Confidentiality, Integrity, Availability (CIA triangle)

Cyber security design principles by the UK National Cyber Security Centre (2019):

- determine all system components (Hardware, Software, Databases, Networks, People & procedures
- Make compromise difficult
- Make disruption difficult
- Make compromise detection easier
- Reduce the impact of compromise

Approaches:

Network security

focuses on networked-resources. Objective is to stop threats from spreading over networks. It is achieved by define and implement access level policies and different types and levels of firewalls such as:

- Packet-filtering

- Circuit-level gateways
- Stateful inspection
- Software
- Hardware
- Cloud

A security access level policies is important to guarantee only necessary access to the different users like Domain, Subdomain, user groups and others.

Software security requirement

General considerations should be:

- Identify: What needs protection from who and for what period.
- Secify: What the system must do and not do and why the system should behave as specified.
- Analyse: How problems must be solve

Some threat modeling techiques:

- Abuse case
- STRIDE
- Attack trees
- Protection trees
- A combination of techniques