Draft 1

Security analysis of large scale computer systems

Introduction

This document is the first draft of the project done for the EP2790 course at KTH Royal Institute. The case that I chose to study for this project is a state-run hospital network computer infrastructure.

1 Phase 0: Scope and delimitations

First of all, it is necessary to define the purpose of the system, the main technical components and what is considered inside and outside of the scope of this study.

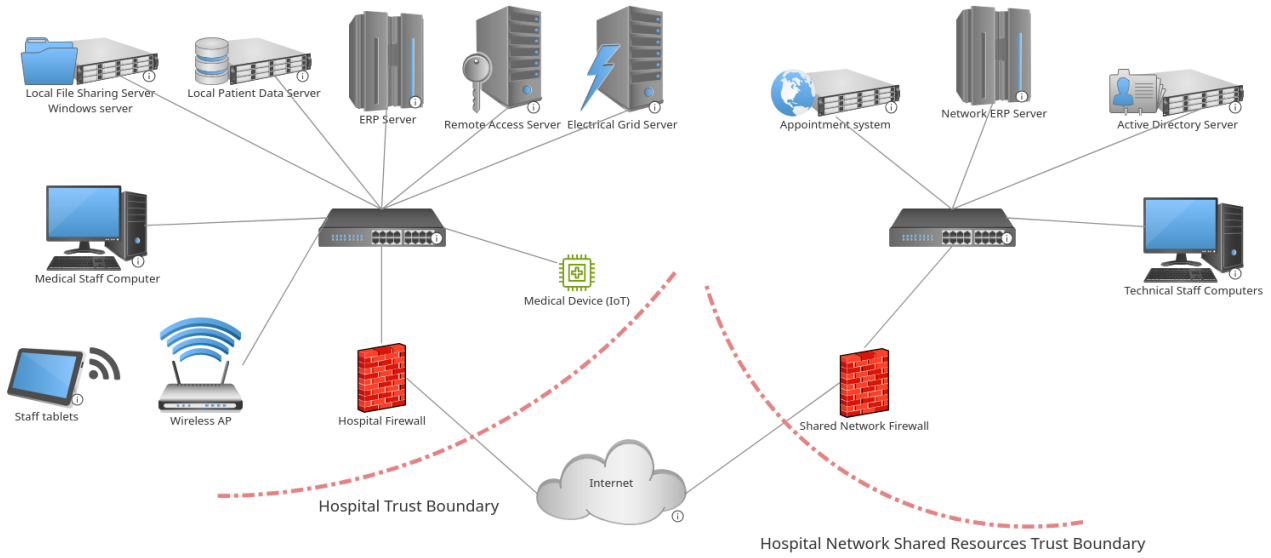

Figure 1: Diagram of the hospital network infrastructure

The Figure 1 represents the studied infrastructure of the hospital network. The resources shared among all hospitals and one hospital network is depicted on the figure. The latter is the same exact copy for every hospitals of the studied network.

1.1 Component description

For the hospital internal infrastructure, there are the following components:

- Hospital Firewall: bridges between the hospital local area network and internet;
- Local file sharing system: enables medical staff to store and exchange files;
- Local patient data server: stores internal medical data of the patients (medical background, stays at the hospital, prescriptions, ...);
- ERP Server: manages the hospital resources (supplies management, in which room is which patient, available beds, ...);
- Remote access server: enables technical staff to access remotely the local area network of the hospital;
- Electrical grid server: manages and optimises the allocation of electricity across hospital as well as backup generator;

- Medical staff computer: enables medical staff to access local area network of the hospital;
- Staff tablets: enables medical staff to access local area network of the hospital through WiFi;
- Wireless AP: enables staff tablets to connect to the hospital local area network;
- Medical devices (IoT): optionally connected medical devices (MRI, scanners, patients monitoring, ...);

And the shared resources infrastructure is made of the following components:

- Shared network firewall: bridges between the shared resources internal network and internet;
- Appointment system: more widely public website of the hospital network that enables the patient to book appointment with doctors and access their prescriptions;
- Network ERP system: manages the network resources between hospital (distributing supplies, managing staff allotment and salaries, ...);
- Active directory server: LDAP server using Microsoft active directory to manage accounts and permissions for staff;
- Technical staff computer: enables technical staff to access shared resources infrastructure and vpn servers of different hospitals;

2 Phase 1: Business analysis

2.1 Business goals

The Figure 2 breakdowns the business goals of the studied organisation, whose main goal is healing the larger number of patients.

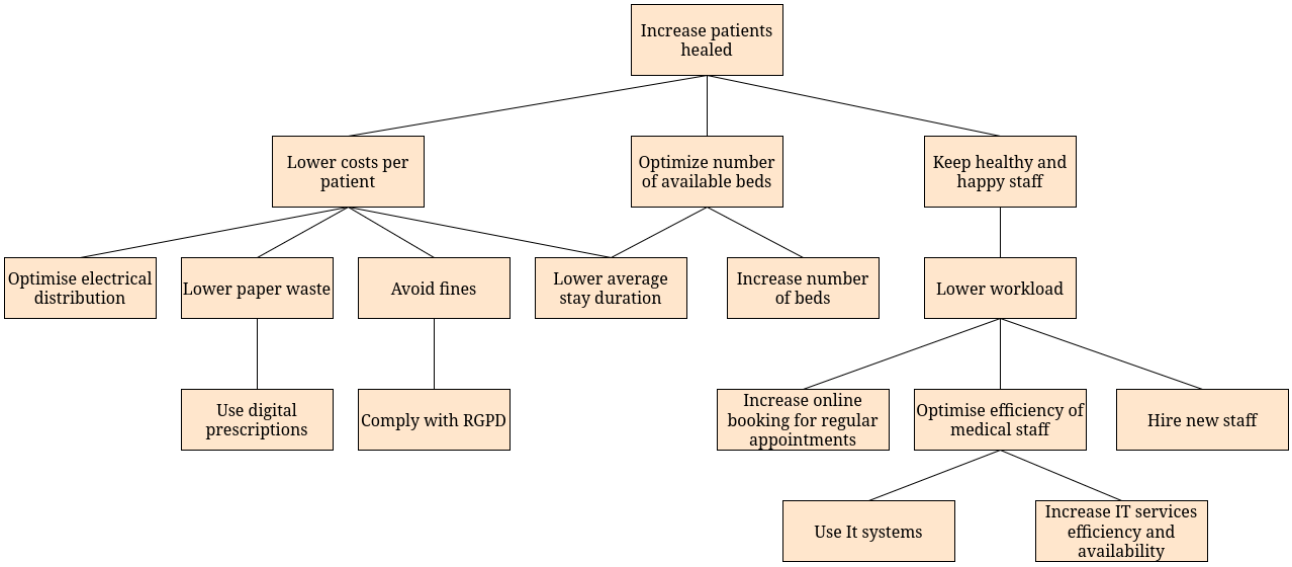

Figure 2: Diagram depicting the business goal of the hospital network

Goals are ordered by importance from top to bottom. A link between two goals indicates that the lower goal serves as a means of achieving the higher goal.

2.2 Business analysis

The Figure 3 highlights the use-cases and links them to actors, goals and assets.

2.3 Loss events

The purpose of this section is to determine the possible loss-events, *i.e.* what could possibly negatively impact the systems and thus the actors in case of attacks.
The Table 1 lists (not exhaustively) the possible loss events that can impact the modelled infrastructure.

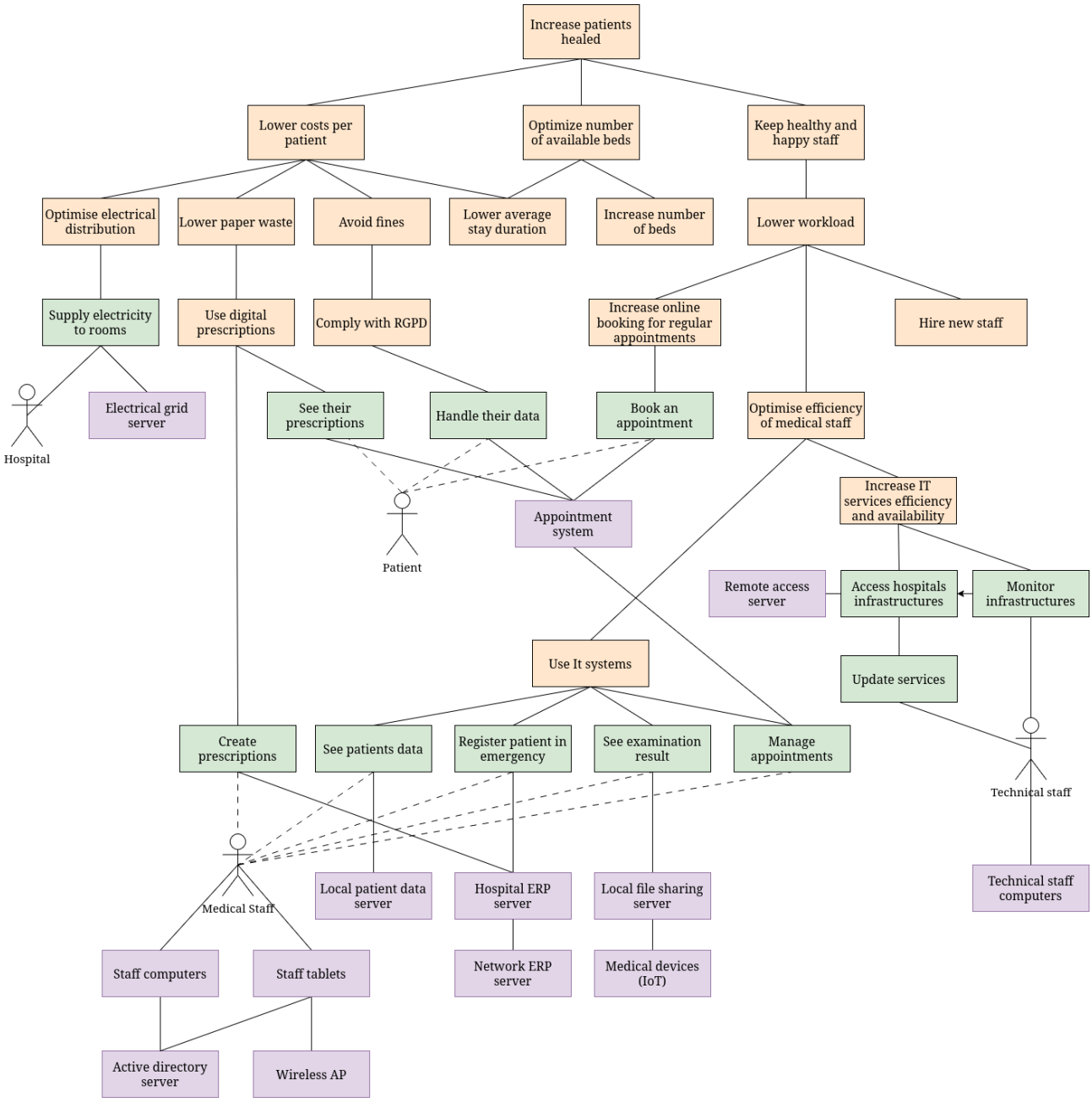

Figure 3: Diagram depicting the use-cases linked to business goals, actors and assets

In orange the business goals, in green the use cases and in magenta assets

3 Phase 2: System definition and decomposition

3.1 List of system assets

The Table 2 and Table 3 list the whole functions assets, respectively, inside the hospital trust boundary and the shared resources trust boundary. The lists provided are quite exhaustives and in the following diagrams, the hardwares and the platform are not distinguished and are depicted as independant trust boundaries if there are more than one service functions embedded in otherwise they are depicted as a function. The flows show interactions between services.

3.2 Data-flow diagram

The Figure 4 describes the data flow inside the studied infrastructure. The flows that crosses the hospital and network shared resources boundaries go through the firewalls of both local networks.

ID	Loss Event	Impacted actor	Type	Magnitude
1	Electrical outage	All	Productivity	10
2	Unavailability of appointment web server	Medical staff and patients	Productivity	5
3	Unavailability of patient data system	Medical staff	Productivity	8
4	Patients data leakage	Hospital network	Fines and reputation	10M€
5	Patients lives endangered	Patients	Injuries/Deaths	10
6	Medical devices replacement	Hospital	Replacement	50k€/200k€/700k€
7	Internal documents leakage	Hospital	Reputation	5

Table 1: Loss events related to actors impacted and their Magnitude
Types are given accordingly to the FAIR method. Two magnitude scales are used, a monetary scale in euros and a discrete 1-10 scale for events that cannot be monetary assessed.

ID	Name	Type
1	Firewall	Hardware
1.1	Pfsense	Service
2	Local file sharing server	Hardware
2.1	Windows server	Platform
2.2	Samba	Service
2.3	File system	Storage
3	Patient data server	Hardware
3.1	Debian	Platform
3.2	Patient data system	Service
3.3	Postgresql database	Storage
4	ERP server	Hardware
4.1	ERP system	Service
4.2	Debian	Platform
4.3	Oracle database	Storage

ID	Name	Type
5	Remote access server	Hardware
5.1	Debian	Platform
5.2	Wireguard service	Service
5.3	Configuration file	Storage
6	Electrical grid server	Hardware
6.1	Debian	Platform
6.2	Electrical grid system	Service
6.3	Oracle database	Storage
7	Wireless AP	Hardware
8	Medical devices IoT	Hardware
9	Medical staff computers	Hardware
9.1	Windows 7 professional	Platform
10	Medical staff tablets	Hardware
10.1	Android 10 and above	Platform

Table 2: List of functions assets inside the hospital trust boundary

ID	Name	Type
11	Appointment server	Hardware
11.1	Debian	Platform
11.2	Apache web server	Service
11.3	Appointment application	Service
11.4	Apache file configuration	Storage
11.5	MySQL database	Storage
12	Network ERP server	Hardware
12.1	ERP system	Service
12.2	Debian	Platform
12.3	Oracle database	Storage
13	Active directory server	Hardware
13.1	Windows server	Platform
13.2	Active directory	Service
13.3	Active directory storage	Storage
14	Shared network firewall	Hardware
14.1	Pfsense	Service
15	Technical staff computers	Hardware
15.1	Windows 7 professional	Platform

Table 3: List of functions assets inside the shared resources trust boundary

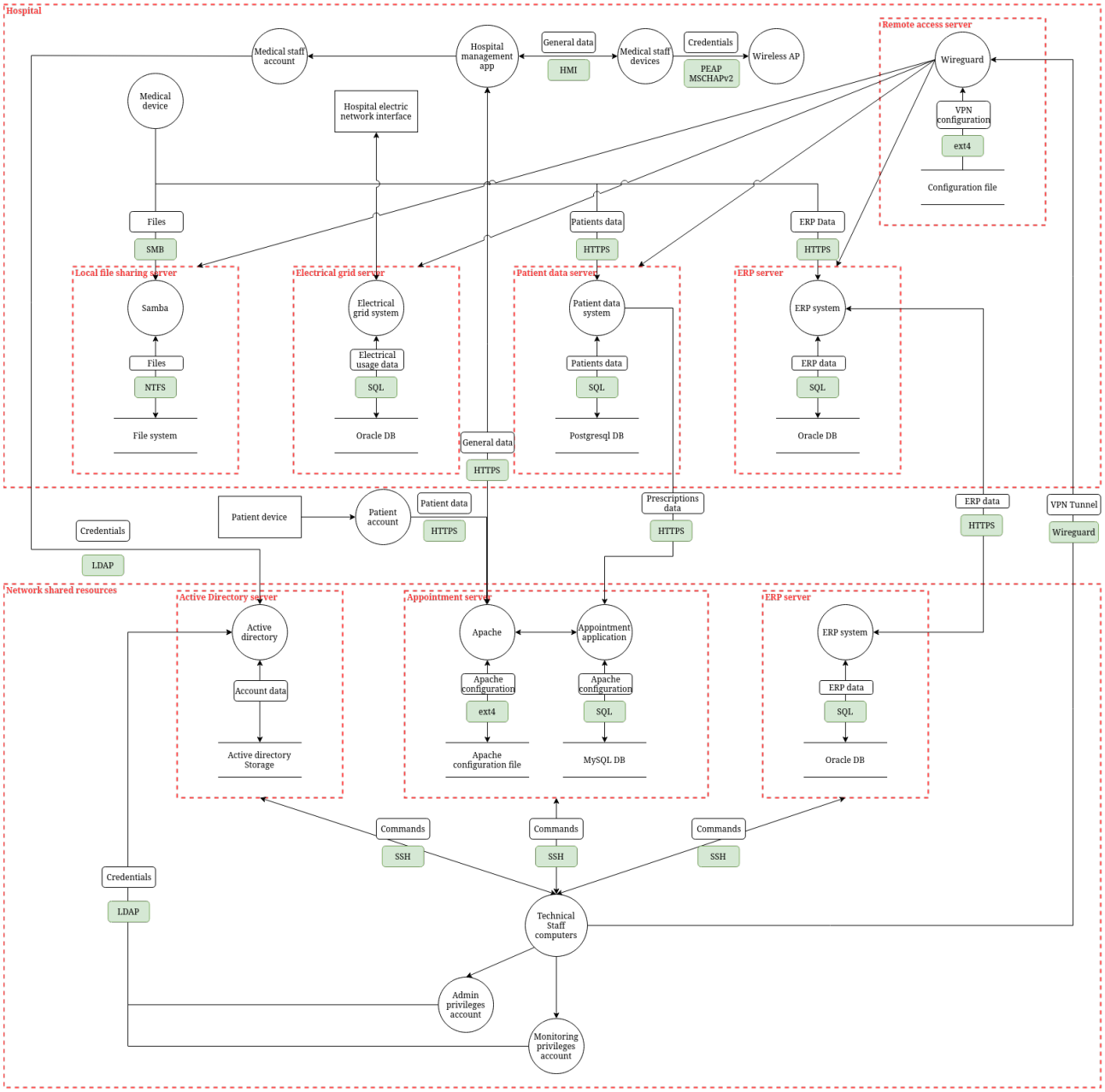

Figure 4: Data flow diagram of the studied infrastructure

4 Phase 3

4.1 Attackers profiles

- Organised crime: groups of hackers motivated by profit of hacking, in this case, this type of attackers will be include in the study;
- Script kiddies: lonely attackers that want to show to their peers their capacity, apply hacking basic logic without understanding everything, this type of attackers will be include in this study also;
- State actors: attackers working for states with support either interrested in profit or unstability in another country, considered in the scope of the study;
- Competitors: other actors in the same field, in our case, there will be out of the scope since this is about health, it is a line that private clinic would not walk;
- Rogue employee: employees that would be entitled to gain a monetary advantage of an attack, has a contact with the infrastructure, also exclude from the scope of this study.