Dennis Thinh Tan Nguyen
01/04/1993
Security
9/6/2017
Stud nr: 0969826792

D1 – Authentication

Since many users may connect to the dispenser, the system must be able to distinguish between the users while still being able to authenticate them. The dispenser may thus store usernames and passwords for the users which they can create. To protect the confidentiality of the passwords each of them is hashed with a random salt.

Also, it is appropriate to utilize an asymmetric encryption (Public key cryptography) scheme such as RSA. The Dispenser will contain a set of public keys where each user has the corresponding private key. For the patients, the private keys are distributed when they sign-up at the hospital and install the application. The corresponding public key is then sent to the dispenser.

For each request, the patients include a digital signature encrypted with their private key which is used to validate the identity of the patient. The digital signature is locally stored on their device which is generated from the application when they install it. Thus, only the device that has the corresponding digital signature may be able to log in; Hence, this may prevent others whom may have access to the credentials to log in from a different device.

Once a patient resigns from the hospital, the app will be removed from their device and the credentials stored in the dispenser will also be removed.

In the event of a patient's private key being stolen by an adversary, one may be able to forge a digital signature. Also, If the adversary also has access to the corresponding credentials, then one may spoof the patient and flood the dispenser with requests. Ultimately, this may prevent the patient from getting their medicine, due to the dosage/frequency limitation being exceeded.

Regarding the nurses, one may not need a digital signature but only need to use login credentials, since it is assumed that only the nurses have access to the wires. Also, it is assumed that the wires have a uniquely defined output jack that can only fit the dispenser and therefore no other than the hospital may own such wire.

Dennis Thinh Tan Nguyen
01/04/1993
Security
9/6/2017
Stud nr: 0969826792

D2 – Risk Analysis

The System

- **Medical Dispenser:** That is the dispenser which may provide medicine to the patients upon request through an app that is connected with Bluetooth. It retrieves patient data from a central database through the internet and can be programmed through a wire that is connected to an iPad.
- **WIFI-Router:** The internet is provided by a WIFI-router which can be connected wirelessly or with an ethernet cable. The routers are managed by an external provider.
- **iPad:** The iPads that the nurses use to access the medical dispenser. It utilizes a unique cable to connect to the dispenser.
- **Internet Connection:** The hospital has a service contract with a third-party internet provider that guarantees network availability of 95.5 %. The internet is over fiber optics and should deliver a bandwidth of 5 Gbit/s
- **Dispenser Wires:** These wires a uniquely crafted for the dispenser and are used to connect to it through the nurses iPads.
- **Patient device with App:** These are the patient's smartphone that has the dispenser app installed. It is used to connect and create requests to the dispenser. If the patient does not own a compatible device, the patient will be provided one for the time stayed at the hospital.
- **Central Hospital Database**: An on-premise Linux database located in the basement of the hospital. The database can remotely be accessed through the internet and is managed by an IT-administrator.

The Stakeholders

- **Patients:** Uses the dispenser to request medicine. Expect to retrieve correct medicine and dosage.
- **Nurses:** They are responsible for the patients and must ensure that the dosage and medicine is correct

Assets and states

Physical Assets

- **Patient's smartphone:** Can be incompatible with app, out of battery or optimal functioning
- **Nurse's iPad:** Can be out of battery, jack-input being broken due to wear or optimal functioning
- **WiFi-Router:** Can be down due to hardware failure or optimal functioning
- **Internet Connection:** Can either be down or available
- **Central Database:** Can be down due to misconfigurations, hardware failures or optimal functioning
- **Dispenser Wires:** Can be broken due to wear, lost or optimal functioning

Logical Assets

- **Patient Records:** Can be incorrect, deleted or correct
- **User Credentials:** Can be incorrect, deleted or correct
- **Digital Signature:** Can be incorrect, deleted, forged or correct
- **Patient App:** Can be outdated, contain breaking bugs or optimal functioning

Dennis Thinh Tan Nguyen
01/04/1993
Security
9/6/2017
Stud nr: 0969826792

Vulnerabilities

Vulnerabilities Affecting Physical Assets: Due to all assets are Electronic equipment, then they may be sensitive to environmental factors. This includes heat, water, pollution, physical shock etc. Except the dispenser wire, they all rely on the availability of electricity to function. All the equipment may break or be damaged due to accidents, by intentions or by wear and tear. The cable and devices may also be lost. Also, the dispenser relies on an active internet connection, so if that is down the dispenser may not retrieve patient data.
Vulnerabilities Affecting Logical Assets: Records can be deleted or modified by accident or by intention. Software used such as App and Database can be misconfigured, outdated or contain bugs preventing them from being used

Threats

- **Employees:** Physical access to dispenser and database.
- **Patients:** Physical access to dispenser and patient device.
- **Hackers:** May access physically or remotely due to dispenser and DB connected to internet.

Risk and Counter measures

The severity of the impact and likelihood of such event happening is based on the categories *high, medium* and *low.* The descriptions of each categories is based on the descriptions illustrated in the course book ("*Applied Information Security – David Basin – P.140*)

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

As such the following risk matrix is created and enables us to infer the resulting risk level for a given impact and likelihood:

Please note that only some relevant assets will be analyzed and not every single asset due to page limit.

Physical Assets: Dispenser Wire					
No	**Threat**	**Planned counter measures(s)**	**L**	**I**	**Risk**
1	Employee: Loose or break	Have additional wires on premise	High	Low	Low
3	Hackers: Steal wire on premise	Ensure wires are not exposed and use surveillance	Medium	High	Medium
Physical Assets: Patient device					
No	**Threat**	**Planned counter measures(s)**	**L**	**I**	**Risk**
1	Employee: Misconfigure	Double checks	Medium	Medium	Medium
2	Patients: Loose or break	Have spare devices	High	Low	Low
3	Hackers: Steal device	Have remote lock of account	Low	Medium	Medium
Logical Assets: Digital Signature					
No	**Threat**	**Planned counter measures(s)**	**L**	**I**	**Risk**
3	Hackers: Forge		Low	High	Low