Unsolvable Solutions
Client: Francois Mouton at the CSIR DSSR

Architectural Requirements

Eavesdropping Protection in Conclave

Github link: `https://github.com/Unsolvable-Solutions/Project-EPIC`

Members:	*Student Number:*
Edwin Fullard	12048675
Jaco Bezuidenhoudt	11013878
Jandre Coetzee	10693077
Maret Stoffberg	11071762
Ryno Pierce	12003922

Contents

1 Introduction

1.1 Project Background

The Android Operating System officially took over the smart phone market in 2010 and it is suspected that about 700 000 Android devices are used in South Africa. It is mostly the corporate or more upper class communities that use these smart phone devices. It is also these individuals who sit in the big corporate meetings where extremely sensitive data can be discussed. For this reason, if these individuals could have eavesdropping malware on their smart phone, it could cause sensitive data to be easily leaked out.

1.2 Project Vision

The Eavesdropping Protection in Conclave (EPIC) aims to protect the integrity of the information discussed during a meeting by eliminating access to the mobile device during a meeting.

1.3 Project Scope

The Eavesdropping Protection in Conclave(EPIC) product consist of a mobile application, a web page, a server, a gateway and a node.

- A meeting is scheduled via the web page. On the creation of the meeting people are invited via email.
- Before the meeting is held, the gateway and node is set up with the list of invited people that may access the meeting room.
- At the meeting, the person opens the application on his phone. He holds the phone over the node, the node then replies if the person has permission to access the room or not. If the person has permission the meeting room is unlocked.
- If access is denied, the gateway sends a refresh request to the server, and the person can try again to gain access.
- When permission is granted, the application will start the protecting mode on the phone.
- The server keeps a log of all the activities. This log can be queried afterwards by the creator of the meeting.

2 Access Channels

2.1 Human Access Channels

2.1.1 Website

The user can access the website via any web browser.

2.1.2 Mobile Application

The user downloads the application on his smart phone. The application is also used to view the meetings that the device is registered to, the user can view these meetings on the application.

3 Architectural patterns

Different structural patterns are used. Some of these patterns stretch over the whole system, while others are just used in parts of the system.

3.1 Layering

The whole system is divided into three layers

3.1.1 Layers:

1. The Presentation Layer
    - The web page
    - The mobile application
2. The Business Logic Layer
    - The Node
    - The Gateway
3. The Data Access Layer
    - The server

3.1.2 Advantages of using the Layering pattern

Pluggability One layer can be replaced or changed, and only the adjacent layers will have to be updated. For example if another server is needed, or if the Android Mobile Application is not enough and a iOS application is needed.

Reusability Since the layers are developed to function relative separately, they can be reused by another system, for example the server or the NFC Node. It is possible for any of the layers to be reused by another system, the code would only have to be adjusted a little if needed.

Testability Since every layer performs its own methods relatively separate from the rest of the layers, unit testing is done very easily. Each of these layers can be tested separately with pseudo input values from the adjacent layers. If the layers perform as it should, they can be tested together.

Complexity reduction All the tasks are divided into the different layers, and therefore the system is simplified. Each layer only has to perform its own tasks.

Maintainability The layers are separate, and are therefore easier to manage and update. It can also be developed by different developers simultaneously.

3.1.3 Disadvantages of using the Layering pattern

High Maintenance Cost If a lower level is changed, the higher level sometimes also need to be adjusted.

Communication Overheads The information could be send unnecessary through many layers. For example when the user scans the mobile device, the email address and password is sends from the phone to the NFC, then gateway, then server, and a respond is send back through the same layers. Now it could be argued that it would be easier for the application to communicate directly with the server, but all the layers in between performs additional tasks in the process, which is needed.

3.2 Model-View-Controller

The server uses a MVC architecture.

Model It is represented by the document orientated database that the server uses.

View The web interface serves as the view.

Controller All the tasks and functions that the user may do via the wep page, like creating a meeting or changing the users of a meeting are the controller.

The usage of the MVC architecture makes the server more maintainable, testable, reusable and simple.
The **maintainability** can easily be seen in the development. Each of the MVC can be developed separately and just be merged afterwards.
The separations of the different concerns makes the **testability** so much easier.

Unit testing can be done and the whole server can then also be tested.
The **reusability** can be seen with the Model, in this case called the database. The database is also used by the Edison for the access control.
The separation of the different concerns shows the **simplicity** of the server.

4 Quality Requirements

4.1 Scalability

- The database on the server can handle up to 819 connections at a time. Therefor up to 819 people can simultaneously use the webpage.
- The node is connected to the gateway via serial USB. Up to three nodes can be connected to one gateway by using a USB hub.
- Only one application can be installed on one phone.
- One user can use more than one phone. This is implemented because phones can be broken and the user could have a temporary phone, or if the user has more than one phone. The user however can only be registered for a meeting with one phone.

4.2 Performance

- The server uses MongoDB for its database. It has been shown that MongoDB can do more than 9000 operations per second. This is clearly a high throughput.
- The response time of the web page relies on the device (computer, tablet or phone) used and the speed of the Internet connection. If both the device and speed of the Internet connection are relatively high, the response time is less than 1.0 second from the server.
- The NFC data transfer time from the phone to the node and back is less than 0.1 seconds. It appears instantly to the user. This is good for the usability, since long scanning may delay the meeting unnecessarily.

4.3 Maintainability

- The code is well documented and each component has a read me file containing all the information on how the functions should be used and what it does.
- Unit tests have been done and are available to view as examples on how the system should be used.

4.4 Reliability

- The server uses MongoDB for its database. MongoDB has a strict concurrent control by using locks. This means that a field may only be updated by one user at a time. This reserve the data integrity, and keep the activity log in order.
- Clustering is used by storing all actions and events in the database.
- The security keeps the data reliable.

4.5 Availability

4.5.1 Application

The application can be downloaded from the github link. Ideally it would later be available on Google play store. See the user manual for installation guidelines.

4.5.2 Web page

The web page is available from any web browser connected to the Internet. The user simply types `projectepic.info` in his favourite browser.

4.5.3 Node

The node used is a Arduino with PN532 NFC/RFID Shield and the lights used are neopixels, it can be purchased from most electronic or robotic online stores. The source code can be downloaded from the github link. See the user manual for installation guidelines.

4.5.4 Gateway

The gateway used is a Intel Edison board and can be purchased from most electronic or robotic online stores. The source code for the gateway can be downloaded from the github link. See the user manual for installation guidelines.

4.5.5 Server

The server uses MongoDB and Node.js. These technologies are freely available online and are very easy to download. See the User Manual for installation guidelines.

4.6 Auditability

- Each action performed on the server is logged in the database with a time stamp. These logs and can be reviewed by the user that owns the meeting at any time. The logs include:
  - A person sends a RSVP for a meeting

  - A person enters a meeting
  - A person exits a meeting
  - A user created a meeting
  - A user invited a person to the meeting
  - A person attempts to enter a meeting, but access is denied.

- During a meeting the application keeps a log of all activities on the mobile device. The log is available for the user to view after the meeting. The log is also uploaded onto the server after the meeting. This is used so the user can see if another application attempted to turn any of the communication mechanisms on.
- A user can view all the meetings that he owns.
- For every event the email and password is tested. This ensures auditability in the event log.

4.7 Security

The system has multiple levels on which security is implemented.

- Between the Node and the phone Near Field Communication (NFC) is used. NFC has its own message protocol called NDEF packaging, and for this you will need a unique ID for each sector you want to read. Plus on the higher (hardware) level you will need to get noticeable close to intercept the message packages, never-mind the strictly one-to-one structure that NFC enforces.
- The Node and the Gateway communicates via a physical Serial connection (a cable). Unless the integrity of the cable is physically compromised or tampered with, the connection is secure.
- Between the Gateway and the server the HTTP protocol is used and this offers sufficient security for this part of the system.
- Then furthermore the system caters for overall security in two ways. The first is the access to the meeting room, so that not just anyone can enter the room. And secondly it stops malware (viruses) from illegally eavesdropping on your meeting.
- AES 128 bit encryption is used when data is send from one source to another.
- The password is stored with MD5 encryption in the database. And if a user object is requested, the password hash is not included in the object. This ensures that if a hacker has breached the firewall, he still cannot get access to the password.

4.8 Monitorability

- The application constantly monitor the state of the phone. It checks if another party has tried to switch on any of the communication mechanisms. If so, the mechanism is turned of again and a notification is send to the user. This is done to prevent malware from turning on the communication mechanisms and sending any information to a hacker.
- When the phone is held over the node, LED lights show the current state of the processing. The LED lights have the following states.

  Blue - Waiting: The node is waiting for a phone to connect with.

  Orange - Processing: The phone has send its information to the node via NFC. The node sends the information to the gateway to check if the user has access to the meeting. And a respond is send back to the application on the phone.

  Green - Access granted: The user may enter the meeting and the phones communication mechanisms are switched off.

  Red - Access denied: The user may not enter the meeting.
- The gateway updates the meeting information every 10 minutes, to see if the list of people attending the meeting has changed.
- The server keeps track of the entering and exiting of meetings, this is used to report any suspicious behaviour. The reporting is done in a log on the server. The suspisious behaviour includes:
  - A person entering but never exiting.
  - A person entering and exiting multiple times.
  - A phones communication mechanisms being turned on during a meeting.

4.9 Testability

- Unit tests are used for each of the functions in all the components. The unit test were manual or automated. The manual testing was done where hardware was involved and where the automated test wasn't possible or applicable.
- The integrations test have been done to combine and integrate all the separate components.
- After the separate components have been integrated, a system test is also performed to test the flow of information and the ovarall usage of the system.
- Usability tests are also to be performed.

4.10 Usability

The system is designed for the users comfort. The user simply has to open the application on his phone and hold his phone over the node to enter a room. His phone is automatically switched to protection mode. After the meeting the user simply has to hold his phone over the node again to exit the room and the protection mode is switched off again.

4.10.1 Application

- The application has a user friendly, clean cut and intuitive interface.
- The application shows clear indications of what tasks could be done and what data should be typed into which fields. This is achieved by descriptive buttons, descriptive labels and clear instructions.

4.10.2 Node

- The node simply has to be plugged into the gateway and it is automatically ready to use.
- The mobile device only has to be held over the node (less than 10 cm) for them to communicate. It is very easy to use.

4.10.3 Gateway

- The user do not directly use the gateway. The gateway sends data to and from the server and to and from the node. The usability of the node however is improved by the fast processing of the server.
- The set up of the gateway for a meeting is very easy to do. The gateway is plugged into a computer and the setup menu automatically runs on the computer. The user then selects a meeting from the list of meetings and the gateway is set up.

4.10.4 Server

The Server is never directly used by the user. The fast processing however do increase the usability of the gateway and the webpage.

4.10.5 Webpage

The website can be used by any device with a web browser.
The web page is made with a very simple clean cut intuitive look. There are three interfaces: The login page, the register page and the homepage.
All the pages on the web page meet the following criteria to enhace the usability:

1. **Clear indications**: The pages shows clear indications of what should be done and what data should be typed into which fields. This is achieved by descriptive buttons, labels and instructions.

2. **Simple navigation**: It is easy to go from one task to another without confusing the user. This is done to improve the performance that relies on the user.

3. **Minimum Visual Cluttering**: Only the necessary tasks are available for the user and no extra information or pictures to distract the user.

4. **Simple font style**: The font colour and style is readable, this increases the usability of the web page.

5. **Simple overall style**: This is use to create a pleasing look and not to bright or visually loud layout.

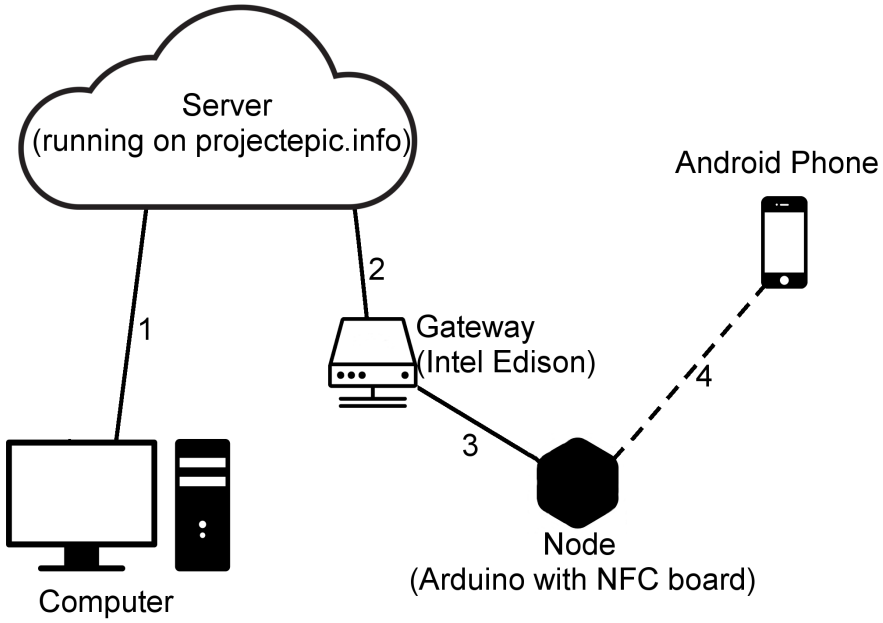
6. **A help function**: If the user is for some reason not sure how to perform a task the help function can assist by showing the set list of tasks available and how to complete them. The help function also provides photos to make the task easier.

7. **Fast**: The web page appear to have complete the task immediately, even though the task may still have to be completed in the background. This is however still dependent on the speed of the Internet connection that the user has.

Note: Usability tests have not yet been done.

4.11 Integrability

The system consists of a mobile application, a node, a gateway, a server and a website. These different part integrate with each other to form one system.



1. The website connects through the Internet via a web browser to the server.
2. The gateway connects to the server via wifi. It relays the data from the node to the server and vice versa.
3. The gateway and node is connected using a cable. It sends the users' information, obtained from the phone via NFC, to the gateway, and transmits results received from the gateway, via NFC to the application on the phone.
4. The phone connects to the node using NFC. The phone sends the users email address, device identification and password to the node, and the node then sends back the response from the server to the application on the phone.

5 Architecture Constraints

- The Mobile application can only be used on Andriod version 4.4 and 5.1. This is because HCE has been introduce from Android version 4.4. These version are currently the only two version above 4.4 which can turn off mobile data automatically (Google removed ability to turn it off in version 5.0.1). There is currently no API (Application Program Interface) that allows developers to turn it off automatically.
- The Node can only communicate with one device at a time.

- The Node can only work if the specific Mobile Application is installed.
- The Edison can only be connected to three Nodes maximum at a time.

6 Technologies Used

6.1 Near Field Communication

Near Field Communication(NFC) is the set of protocols that enable electronic devices to establish radio communication with each other by touching the devices together, or bringing them into proximity to a distance of typically 10cm or less. Unsolvable Solutions have decided to use this technology for the following reasons:
The reasons for using this technology are:

- Client requirement specification
- This method is more secure than other communication methods, because it requires the devices communicating to be less than 10cm apart. This enables one to monitor the users that communicate via NFC.

6.2 Node.js

Node.js is an open-source, cross-platform runtime environment for developing server-side web applications. Node.js applications are written in JavaScript.
The reasons for using this technology are:

- It works well with MongoDB
- Personal preference.

6.3 Arduino

Arduino is an open-source computer hardware and software company, project and user community that designs and manufactures microcontroller-based kits for building digital devices and interactive objects that can sense and control the physical world.
The reasons for using this technology are:

- Supports NFC

6.4 MongoDB

MongoDB is an open source, document-oriented database designed with both scalability and developer agility in mind. Instead of storing your data in tables and rows as you would with a relational database, in MongoDB you store JSON-like documents with dynamic schemas.
The reasons for using this technology are:

- It has fast processing.
- Open source.
- Previous knowledge.
- Personal preference.
- Flexibility.

6.5 Java

Java is a programming language expressly designed for use in the distributed environment of the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces an object-oriented programming model.
It is used in conjuction with Angroid SDK.

6.6 Android SDK

A software development kit that enables developers to create applications for the Android platform. The Android SDK includes sample projects with source code, development tools, an emulator, and required libraries to build Android applications.
The reason for using this technology are:

- All application created for Android need to be done through the Android SDK.

6.7 Host Card Emulation

Host Card Emulation (HCE) is the term describing on-device technology that permits a phone to perform card emulation on an Near Field Communication (NFC)-enabled device without relying on access to a secure element
The reasons for using this technology are:

- In order for an Android device to send a data via NFC to a non-Android device, we needed to emulate a NFC tag. HCE allows us to emulate a universal NFC tag that is readable by almost any device that can process NFC messages.

6.8 JavaScript

JavaScript is most commonly used as a client side scripting language. This means that JavaScript code is written into an HTML page. When a user requests an HTML page with JavaScript in it, the script is sent to the browser and it's up to the browser to do something with it.
The reasons for using this technology are:

- It is easy to use with Node.js and MongoDB
- It is freely available.
- It is a very powerful and flexible language.

6.9 AngularJS

AngularJS is a structural framework for dynamic web apps. It lets you use HTML as your template language and lets you extend HTML's syntax to express your application's components clearly and succinctly. Angular's data binding and dependency injection eliminate much of the code you would otherwise have to write.
The reasons for using this technology are:

- It is easy to use with JavaScript, Node.js and MongoDB
- It is freely available.
- It is a very powerful and flexible language.

6.10 Intel Edison

The Intel Edison is a tiny computer offered by Intel as a development system for wearable devices. The system was initially announced to be the same size and shape as an SD card and contain a dual-core Intel Quark x86 CPU at 400 MHz communicating via Bluetooth and Wi-Fi.
The Intel Edison is used as the gateway. The reasons for using this technology are:

- The two options for the gateway was using the Intel Edison or using the a Raspberry Pi. And even though the Raspberry Pi was cheaper (R550), the Intel Edison(R1666) has built in wifi.
- The Intel Edison was sponsored by Intel for the project.