Project Proposal

Natalie Jablonsky, Matthew Leeds, Oliver Necovski

Contents

Introduction

Mobile devices are being used more than ever with billions of messages sent every day. The risk of message interception has never been greater.

Throughout this project we will use an Arduino microcontroller paired with other accessories to allow us to encrypt SMS messages. This will allow us to send sensitive data from the Arduino to a mobile or another device and decrypt using a shared key or another form of cryptography. This document will highlight our plans to approach the project.

Project Outline

This project encompasses the use Arduino hardware to encrypt/decrypt SMS messages. The device will consist of an Arduino using 2G module with an LCD screen to display messages. The software to control the Arduino will be developed within the Arduino IDE using C/C++. The encryption system is chosen by us and can be an existing protocol or of our own creation. There is also an opportunity to extend the project to utilise regular smartphones.

Software

For coding the software that our team will be utilizing for our sms encryption/decryption service will be the open-source Arduino Software. Our reasoning behind this choice is due to a number of factors such as cost, ease of use and compatibility. The open source software is compatible with multiple operating systems. Which is ideal as our group consists of people who use the Windows and Mac OS.The software also works with all types of Arduino boards which clears any possible problems with compatibility. Another reason why we have selected this software is that the programming can be done in C and C++ (Arduino 2016), which plays to our groups skill sets.

Overall the software is ideal for our projects needs and the fact that it is open-source means means that we will be eliminating any software costs.

Hardware

Arduino boards are cost effective open source microcontrollers which allows them to be used as digital building blocks. Adding modules for I/O functionality and programming for commands make them a powerful tool for DIY projects, including; motors, robots, communication devices and other useful tools.

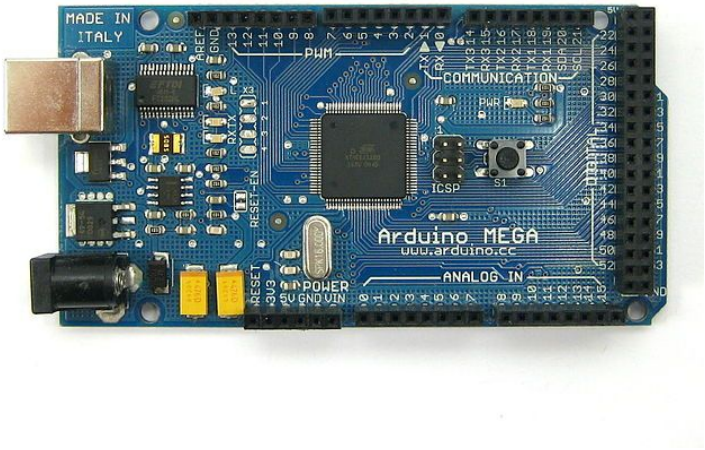
This project allows us to use Arduino boards with extra modules to create our end product.
We will be using:

Arduino, MEGA 2560 board

- Arduino compatible LCD screen 20 character 4 lines with IIC 4 pin serial input
- Arduino GSM/GPRS Shield.
- Power Supply
- Micro-SD card

- USB a/b
- Connected Windows/Linux/ MAC Computer

Our hardware will interact with the software on the computer allowing us to program the board and output to the display any necessary information. These devices are not built as a complete unit. We will need to solder and wire certain areas of the board to allow it to function as we want.
(Arduino, 2016)



Development Environment

The areas of Information Technology that this project uses are:

- Security
  - The goal of this project is to encrypt and decrypt SMS messages.
    We are using cryptography to ensure that the messages are securely encrypted and possible to decrypt using the correct algorithm.
- Communications / Networking
  - Arduino supports a GSM mobile networking shield which allows us to connect the device to a network. This will allow us to send the encrypted message to another network connected mobile device.
- Programming
  - Arduino board requires programming to allow it to function correctly. The board needs to be able to communicate with the computer as well as communicate with

other I/O modules. This is done via programming the internal memory and the SD card to achieve the desired outcome.

Functions

Upon completion of the project we aim to have a prototype that will be able to send and receive sms messages securely over the 2G network. These messages will be encrypted and decrypted via an algorithm that will be developed by the project team. This algorithm will undergo numerous testing to make sure that it is secure and suitable for its purpose.

For this project we will be using devices that are not practical to carry around, however it would be suitable to set up in a home or office environment in order to establish a secure communications channel. As we are producing a prototype, further development could lead to a smaller and more portable solution.

Research & Investigation

There are many different types of cryptographic systems currently being used for different purposes, though these systems may be private and run on many different platforms they may have vulnerabilities.

iMessage

From Apple uses a 128 bit AES encryption. These messages are encrypted by using 2 sets of private and public keys. One is used for encrypting the message and one is used for signing or authorising the message. The private keys are stored on the device and are not visible to anyone. This is a high security protocol which allows low risk of data loss or stolen data.

KNOX

From Samsung is a security feature for samsung devices, it allows some applications to be used within a security layer of the phone secured by a 256 AES encryption between the client, transmission and servers. KNOX messaging is an application that can be used within this layer which can transfer messages to other KNOX messaging users.

Arduino

Arduino microcontroller encryption. As these devices are open-source there are many users who have previously experimented with using encryption for sms creating their own 128 and even 256 AES encryption between 2 devices. This ranges in complexity. Sharing the private key over different platforms then sending the encrypted message from one device to another and using the private key to decrypt it. Creating a public key which is able to generate individual private keys depending on who the messages are sent too.

SMS

SMS encryption. Currently sms encryption is managed by a message being sent over a radio signal between the phone and the mobile tower, Devices are able to be created which can replicate a mobile tower signal which is able to reveal a text message. This is not safe at all. Although if we encrypt this message on the sender's end and was intercepted it would be unreadable by any hackers.

After researching some different examples of encryption for many platforms we will investigate further into AES, RSA and other Key based encryption services that will work for our Arduino Microcontroller which will allow us to send an encrypted message from one Arduino Microcontroller to a phone or another Arduino.

Furthermore Jemal has provided his paper “Security Considerations for Wireless Carrier Agnostic Bio-Monitoring Systems” to give us some motivation and possible application for our system.

Methodology

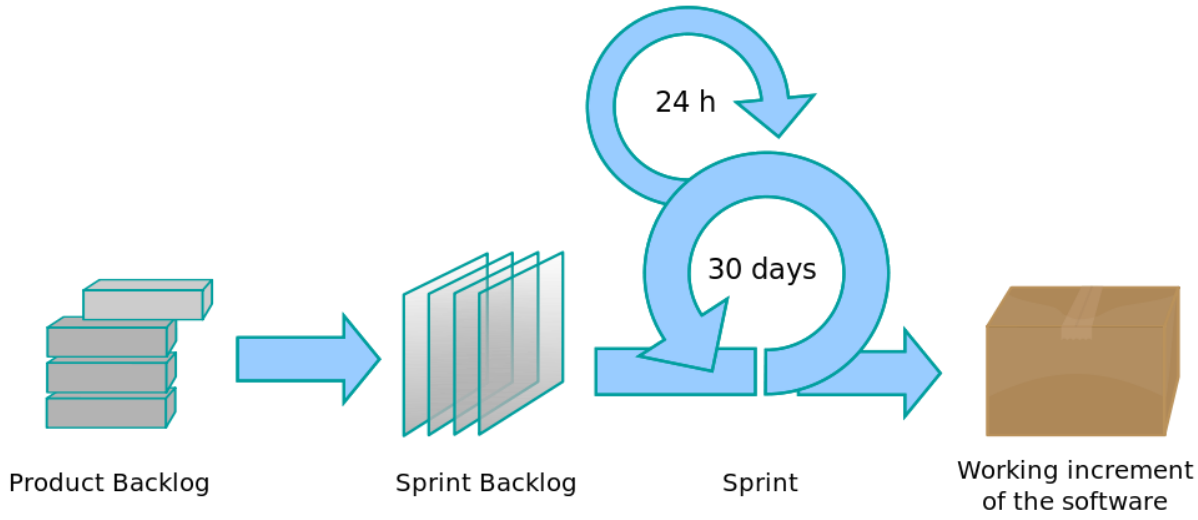
GIven the scope and requirements of the project, the methodology we are choosing to adopt is an agile approach using the Scrum method.

For some background, agile software development focuses on these four core values (Agilemanifesto.org, 2016):

- Individuals and interactions over processes and tools.
- Working software over comprehensive documentation.
- Customer collaboration over contract negotiation.
- Responding to change over following a plan.

The Scrum method feeds upon these values and creates a framework that help us in completing this project. The workflow of Scrum is rather straightforward as mentioned by (Schwalbe, 2014, pg 70):

- A product owner (in our case the Jemal) creates a list of tasks called the product backlog.
- Next the development team (us) will begin sprint planning by choosing a portion of the tasks to implement from the product backlog. These chosen tasks form the sprint backlog.
- The development team then allocates a certain amount of time (the sprint) to complete the sprint backlog. The sprint can last from 2-4 weeks with daily meetings (daily scrum) to assess progress.
- During the sprint the Scrum Master (for us the leader of the group) keeps the development team on focus.
- At the end of the sprint the product should be functional. Furthermore, the development team reviews the sprint and add any issues to the product backlog.
- And the process repeats when the development team chooses tasks from the product backlog.



(Lakeworks, 2009)

Further information can be found at (Scrumguides.org, 2016).

We have chosen this approach because the requirements for the functionality of the project are ambiguous which could lead to potential changes further into development. Also, using iterative and incremental sprints allows us to regularly receive feedback from our supervisor Jemal and in turn improve the quality of the final product. Furthermore, during development this methodology could help us identify issues early on in the process.

System Analysis and Design

When managing data certain security plans must be set in place in order to protect privacy. As messages will be sent to and from the Arduino board, any data that travels through the network may be at risk as it might be stored on the arduino board. For this reason any data that is being sent over the network will be deleted after a certain criteria is met. This criteria could be based on the amount of messages stored or a time limit.

The programming within the project will follow the following process:
A message will be sent to the arduino board via a computer, once the board receives the message it will be encrypted via the encryption algorithm that has been programmed on it. After the message is encrypted, it will then proceed to be sent to another mobile device. Before that device receives the message, it will first need decrypted. The decryption will either be handled via another Arduino board or another method. Once the message is decrypted, A message will be displayed on the mobile device. We aim to break this process into two parts; encryption and decryption, in order to produce a suitable solution.

Implementation

The Arduino microcontroller is our gateway to the network, with easily accessible hardware and open source software this makes it the perfect equipment to achieve our goal.
The Mega 2560 and its GSM Shield allow us to make a connection between our computer, open source software out to the GSM network allowing us to send SMS messages.
These messages can be altered with the programming of the software and run through algorithms before being sent. Our algorithms will contain Crypto keys allowing the messages to be scrambled and unreadable if they were to be intercepted. Using these keys in reverse will allow the message to be decrypted and in a readable format.

Documentation

Software Documentation

Documentation covering the usage of the device, standards, protocols and encryption methods used, as well as interactions between hardware and software components will be created to allow users to become familiar with the operation of the product. Furthermore, notes on the following will also be recorded:

- Logs of any changes made.
- Backups of previous solutions.

Our Communications

- Project updates posted to a group Trello board.
- Meeting with Jemal on March 17, established the project requirements and acquired approval.
- Skype conference on March 18, assigned roles, discussed specifics on how to develop the system.

Presentation

Given that Greg provides us with the opportunity to present to class, we can use this to practise for the final presentation (Assignment 4) as well as inform the class of our progress.

Our presentation will focus on these following areas:

- Our Roles
- Planning and schedule
- Deliverables
- Supervisor interactions/communications
- Testing

The presentation will aim to present how we applied our skills to create a project that meets our supervisor's expectations.

Reflection

For self-reflection, each week us, individually, are encouraged to write a reflection outlining our experiences working on the project. Because these reflections are required for Assignment 5, taking this approach will hopefully allow for high quality reflections and identify issues within the group early on.

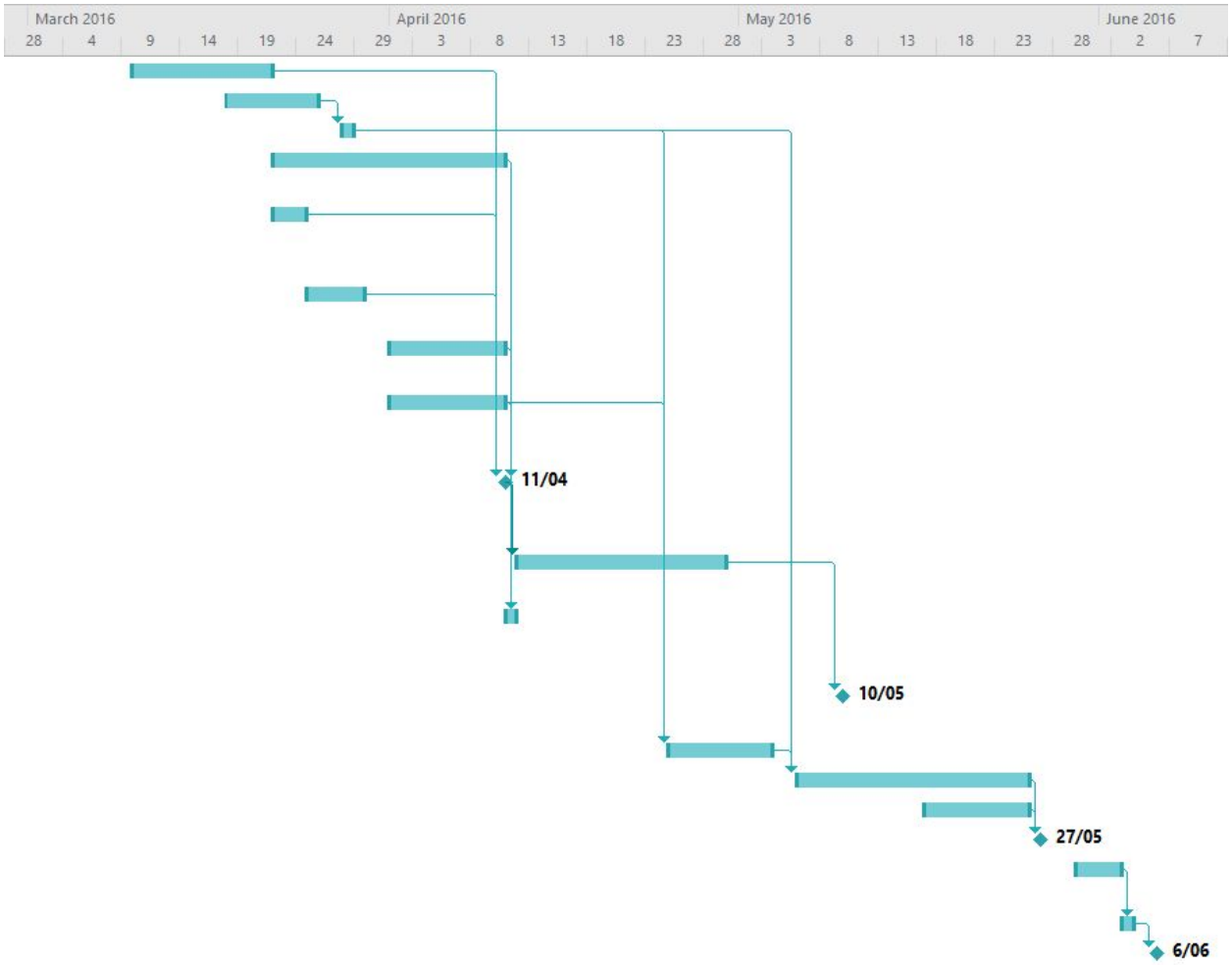
Our Roles

Our project will consist of 4 defined roles. Cryptography will deal with the design of a cryptographic protocol for the Arduino. Documentation entails documenting the project. Programming handles the development of the software. Research will investigate cryptographic systems, similar devices, and hardware. As the project progress we may assist each other depending on the difficulty or complexity of the task.

Role	Member
Cryptography	Oliver
Documentation	Stephen
Programming	Natallie
Research	Matt

Timeline/Gantt Chart

	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		Project Proposal	8 days	Thu 10/03/16	Mon 21/03/1	
2		Purchase Hardware	6 days	Fri 18/03/16	Fri 25/03/16	
3		Assemble Hardware	1 day	Mon 28/03/1	Mon 28/03/1	2
4		Research/Investigati Report	15 days	Tue 22/03/16	Sun 10/04/16	
5		Research Existing Encryption Solutions (iMessage, myKnox)	3 days	Tue 22/03/16	Thu 24/03/16	
6		Analyse 2G GSM Protocol	3 days	Fri 25/03/16	Tue 29/03/16	
7		Study Arduino Development	7 days	Fri 1/04/16	Sun 10/04/16	
8		Study Encrytion Algorithms and Methods	7 days	Fri 1/04/16	Sun 10/04/16	
9		Research and Investigation Report Due	0 days	Mon 11/04/16	Mon 11/04/16	1,4,5,6,7,8
10		Analysis and Design Report	14 days	Tue 12/04/16	Fri 29/04/16	9
11		Determine Suitable Encryption Algorithm	1 day?	Mon 11/04/16	Mon 11/04/16	8
12		Design Stage Complete	0 days	Tue 10/05/16	Tue 10/05/16	10
13		Program Arduino	7 days	Mon 25/04/1	Tue 3/05/16	3,8
14		Test Product	14 days	Fri 6/05/16	Wed 25/05/1	3,13
15		Document Product	7 days	Tue 17/05/16	Wed 25/05/1	
16		Project Delivery	0 days	Fri 27/05/16	Fri 27/05/16	14,15
17		Presentation Preparation	4 days	Mon 30/05/16	Thu 2/06/16	
18		Presentation	1 day	Fri 3/06/16	Fri 3/06/16	17
19		Project Conclusion	0 days	Mon 6/06/16	Mon 6/06/16	18



Testing

As we are using agile techniques we need to implement testing throughout our sprints to ensure our software is reliable, secure and functional. Because we are dealing with encryption it is paramount for us to verify that our chosen cryptographic system is hard to attack. Furthermore we need to test:

- Sending a SMS
- Receiving a SMS
- Encrypting/Decrypting a SMS
- That hardware is interacting correctly
- That the device is secure from attacks

The testing process as described by (Schwalbe, 2014, pg 333-335) will be made up of four phases:

- Unit Testing - Involves testing each individual component (hardware and software) of the device. This ensures that each component is bug-free and performing correctly.

- Integration Testing - Involves testing a group of components, eg. The encryption components both hardware and software. This ensures that components are interacting correctly with each other as well as verifying that subsystems are functioning.
- System Testing - Involves testing the whole device with all components working together. Obviously this is to ensure that the whole system is functioning properly and at the stage to be used by end users.
- Acceptance Testing - involves the final testing of the solution to ensure that it meets requirements for the supervisor. This phase of testing does not deal with technical issues, that should've been done in System testing.

Conclusion

The project aims to to construct a 2G/3G SMS encryption system using Arduino hardware. We will be using purchased Arduino hardware, the Arduino IDE and Libraries to develop our solution. We will investigate similar systems as well as existing encryption systems. For development we are adopting the scrum method to develop the application. This is to ensure that we are able to produce a fully functional device meeting the requirements of the project. Furthermore, we have set up processes to ensure quality, organisation and teamwork.

References

Arduino 2016, "Arduino", retrieved 18 March 2016, <https://www.arduino.cc/>.

Arduino 2016, "Can I program the Arduino board in C?", Arduino, retrieved 18 March 2016, <https://www.arduino.cc/en/Main/FAQ>.

Scrumguides.org 2016, "Scrum Guide", retrieved 18 March 2016, <http://www.scrumguides.org/scrum-guide.html>.

Lakeworks 2009, "Scrum process - Wikimedia commons", retrieved 19 March 2016, < https://commons.wikimedia.org/w/index.php?curid=3526338>.

Schwalbe 2014, Information Technology Project Management , 7th edn, Course Technology, Boston, USA.

Agilemanifesto.org 2016, "Manifesto for Agile Software Development" retrieved 18 March 2016, <http://agilemanifesto.org/>.

Tech Crunch 2014, "Apple Explains iMessage", retrieved 19th March, 2016 <http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/>

Clove 2013, “What is samsung KNOX”, retrieved 19 March, 2016 <http://blog.clove.co.uk/2013/10/22/samsung-knox/>

ResearchGate 2014, “Cryptosystem based on Arduino Microcontroller”, retrieved 19 March 2016 <https://www.researchgate.net/publication/264842603_A_Tiny_RSA_Cryptosystem_Based_On_Arduino_Microcontroller_Useful_For_Small_Scale_Networks>

StackOverflow 2015, “Intercept SMS Messages”, retrieved 19 March, 2016 <http://security.stackexchange.com/questions/11493/how-hard-is-it-to-intercept-sms-two-factor-authentication>