

Electronics and Computer Science
Faculty of Physical Sciences and Engineering
University of Southampton

Matthew Hutchings
5th of May 2020

Recommending and modelling optimal security practices for smart grid connected IoT devices

Project Supervisor: Dr Nawfal Fadhel
2nd Examiner: Dr Xu Fang

A report submitted for the award of
MCOMP Information Technology in Organisations

Contents

1	Project Description	4
1.1	Project Aims and Objectives	5
1.2	Project Scope	5
2	Literature Review	6
2.1	Internet of Things (IoT) Devices	6
2.2	Smart Grids	6
2.3	IoT Smart Grid, the Threats, Attitudes and Best Practices	6
2.4	Verification of Security Policies and Protocols	7
3	Research and Design	8
3.1	Threat Model	9
3.1.1	Weak/Default Password Fuzzing Attack	10
3.1.2	Man In The Middle (MITM) Attack	10
3.1.3	Passive Eavesdropping	11
3.1.4	Replay Attack	11
3.1.5	Impersonation Attack	12
3.1.6	Open Port Scanning	12
3.2	Recommendation of policies and practices	13
3.2.1	Policy List	13
4	Implementation and specification of non-communication IoT policies	14
4.1	Smart Hub password management	14
5	Implementation and modelling of communication protocol policies	15
5.1	Message Encryption	15
5.1.1	Design	15
5.1.2	Implementation	16
5.1.3	Review	17
5.2	Unique Session Keys	18
5.3	Unique Session Keys	18
6	Plan for remaining work	18
6.1	Risk Analysis	18
6.2	Gantt Chart	19

Statement of Originality

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

I have acknowledged all sources, and identified any content taken from elsewhere.

I have not used any resources produced by anyone else.

I did all the work myself, or with my allocated group, and have not helped anyone else.

The material in the report is genuine, and I have included all my data/code/designs.

I have not submitted any part of this work for another assessment.

My work did not involve human participants, their cells or data, or animals.

1 Project Description

IoT devices present many exciting applications for both industrial and consumer use. However, increased dependence on these devices opens up new consequences and attack vectors that an adversary can use to attack a target. This is of particular importance in the case of IoT devices connected to smart grid infrastructure as cyberattacks could be used to disrupt critical national infrastructure.

The scenario for my project is a IoT based smart grid with a focus on the IoT devices in the system and their interactions with the cloud layer.

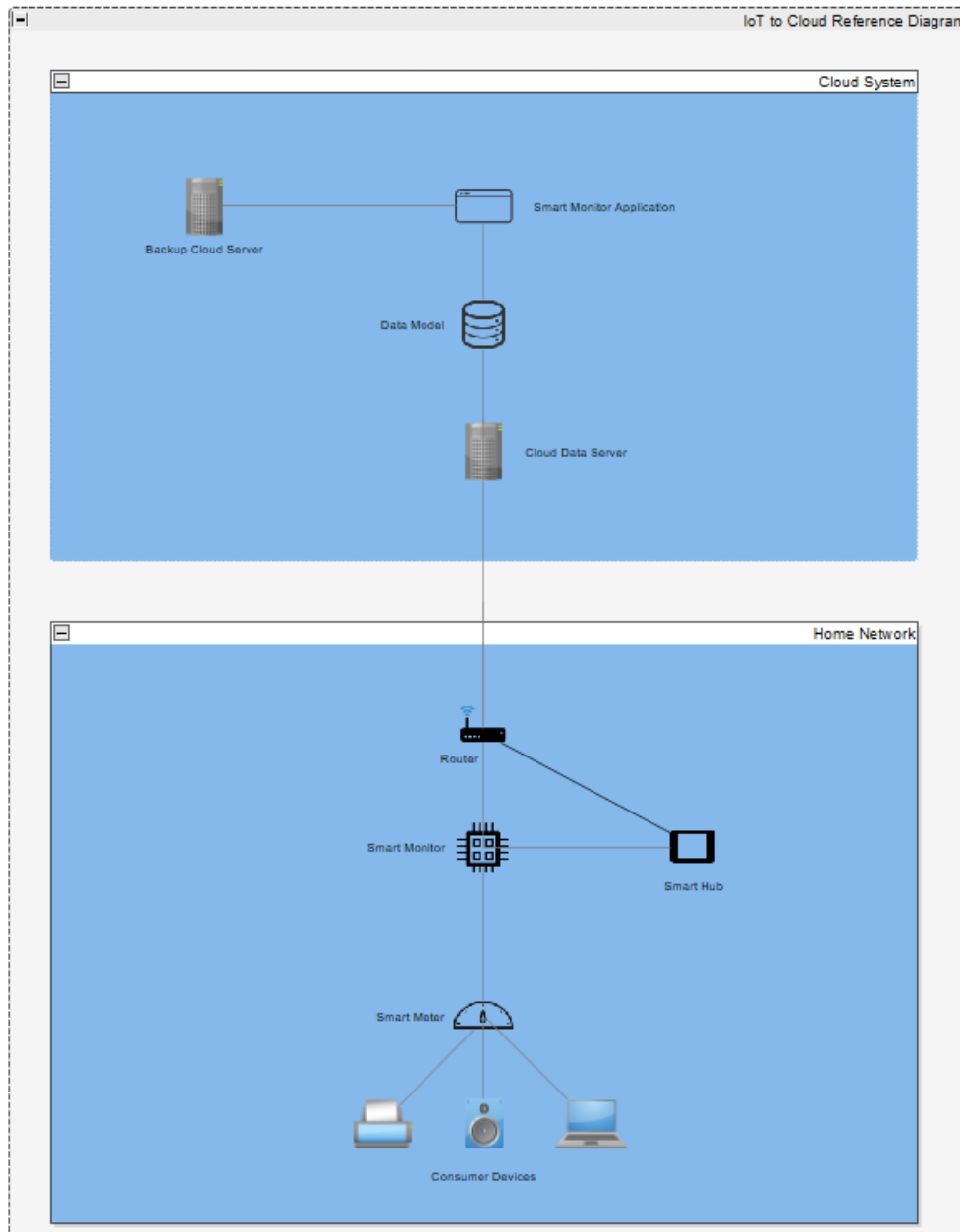


Figure 1: Reference diagram of my smart grid scenario

1.1 Project Aims and Objectives

This project aims to produce, model and verify a collection of policies and protocols that are suitable for mitigating the threats that a IoT enabled smart grid may face. I wish to focus on the following goals within this project:

- Investigate and conduct a risk assessment on the main vulnerabilities and threats faced by IoT devices within smart grid environment.
- Recommend security policies that can mitigate these threats, justifying these policies by taking into account secondary factors including the cost to implement and any loss to productivity these policies might incur.
- Implement and verify that these communication protocols mitigate the identified vulnerabilities using Scyther, a formal method based protocol verification tool.
- Clearly explain the impact of each of my policies by comparing the possible attack vectors with and without each policy using Scyther.
- Create a purpose built, portable Scyther virtual machine environment allowing myself and others to quickly set up and start using Scyther on a new device.

1.2 Project Scope

The scope of this project will be investigating, modelling and verifying the best policies and practices for IoT devices and their communications in my smart grid scenario. The project will focus mainly on IoT communication protocols and their configuration rather examine flaws in the hardware or firmware ran by these devices.

2 Literature Review

My literature review explores the IoT and smart grid landscape before looking into the cybersecurity issues that a smart grid implementation may face. Finally, the review discusses the verification of cryptographic protocols in the context of my scenario.

2.1 Internet of Things (IoT) Devices

IoT as a general concept can be described as physical objects also being network identifiable devices that are able to communicate without the need for human interaction [1]. These devices can be used in a home or industrial context to automate processes or afford additional functionality. IoT devices can do this as they are able to leverage information by collecting/receiving it across a network. As an example of an IoT implementation in a chemical production plant, IoT monitoring devices could be used to monitor the temperature of a reaction. If the temperature fell outside of the requirement, the device could communicate with another IoT device that controls the coolant flow through the reaction and correct it without the need for any human interaction.

These IoT networks can offer benefits for existing processes such as improved efficiency, fewer employees required to manage it and data which can be used to improve the process. However, it is important to consider from a cybersecurity perspective that the introduction of networked devices to a process opens it up to the possibility of cyberattacks.

2.2 Smart Grids

The term smart grid refers to the integration of technology into electrical grid systems allowing them to dynamically change to meet the current needs of consumers [2]. Whilst the implementation of smart grids can vary significantly, several elements generally remain constant:

- **Smart Meters and Monitors** - These IoT devices are used to measure and analyse the energy usage within a single home. Typically smart meters simply collect energy readings from a room and send this information to the smart monitor. This monitor relays energy information to a collection server and receives information on current energy prices. [3]
- **Smart Hub** - This device allows the homeowner to track their electricity usage as well as view the current electricity price to help time their electricity usage to get the best price resulting in a better distribution of power demand across the power grid.
- **Cloud Layer** - This layer communicates with the Smart Meter to receive electricity usage information and send electricity pricing information. This information can then be used by the rest of the smart grid system to adjust the routing and production of electricity based on current demand.

2.3 IoT Smart Grid, the Threats, Attitudes and Best Practices

A key finding from my research, summarised by Robles [4] is that one of the key differences between securing a traditional system compared with a national infrastructure system, such as smart grid, is the reduction in the effectiveness of standard security measures such as patches, password management and access control. Stating that this is due to the size and diverse combination of hardware and software that comprises this class of system. Whilst traditional controls do have their place in smart grid security Sajid [5] identifies the need for specific security measures that directly mitigate the threats smart grids face. This point is further explored by Bere [6] which states that large industrial control systems are often the target of state-funded Advanced Persistent Threat (APT) groups whose capabilities and resources far outmatch the typical threat actors a system faces. [6] Bere goes on to recommend that the security protocols and controls implemented should be layered, providing a 'defence in depth' security approach which Virvilis [7] states as a key countermeasure against APT groups as these groups have the ability to execute zero-day exploits. Zero-day exploits offer very little chance

of mitigating an attack against part of a system as the vulnerability is only known to the adversary at the time of execution [8]. However, a layered system means that in the event of such an attack, the entire system will not be compromised due to the presence of other security measures and protocols.

Another area of difficulty when it comes to securing these systems is the perspective and attitudes of governments and other organisations when it comes to securing these systems. Wang [9] states that many organisations do not see investing in the protection of these systems as economically viable. Virvilis [7] adds that disruption to productivity and user experience due to the increase in latency or removal of features that hardened security protocols may necessitate is another factor in the lack of implemented protocols on these systems. McQueen [10] suggests that it is difficult to quantify cyber risk using traditional risk assessment methods. This may further contribute to the reluctant attitude towards cybersecurity investment as it is difficult to quantify the reduction in risk to management.

2.4 Verification of Security Policies and Protocols

Creamers [11] states that it is very difficult for humans to analyse and find flaws in cryptographic protocols, as evidenced by the number of protocols that are found to have security flaws after their release. An example of this is the Needham-Schroeder key distribution protocol which even after extensive analysis and verification by hand was found to have a security flaw which allowed an adversary to pass off an old session key as a new and valid one [12]. Meadows [12] goes on to suggest that formal methods are a good choice for analysing these cryptographic protocols as they are enclosed enough to make modelling and verification feasible whilst also having the potential for subtle and counter-intuitive flaws that an informal analysis may miss.

In order to verify a protocol using automated formal methods, it must first be modelled so that it can be interpreted by a protocol verification tool. In my research, I have found two tools that are the most suitable for this purpose; Pro-Verif and Scyther. In their comparative analysis of these two tools Dalal et al. [13] identifies that whilst the two tools share several similarities, there are several differences that make Scyther more suitable than Pro-Verif for my scenario and skillset.

- **Modelling Language** - Scyther uses 'security protocol description language' (SPDL) described as "a mix between java and C" by creator Cas Creamers [11] to model protocols. Whereas Pro-Verif protocols are represented using horn clauses or pi calculus [13]. The SPDL used by Scyther is closer to pseudo-code than Pro-Verif making it more suitable for illustrating the implementation of protocols as well as being more fitting to my skillset.
- **Attack Graphs** - Scyther automatically generates attack graphs when a flaw is found in verification, generating a visual flow diagram of the attack. Pro-Verif does not support this feature.

Based on these factors, the project will use Scyther for the modelling and verification of protocols.

3 Research and Design

When it comes to implementing a best practice cybersecurity strategy, NIST [14] recommends a five step process for analysing and securing smart grid systems:

- **1. Defining use cases** - The use cases of the system should be defined. This project defines use cases through the reference diagram.
- **2. Risk Assessment** - The vulnerabilities, threats and the impact these threats can cause should be evaluated for the system. This project performs a risk assessment through the threat model and threat descriptions.
- **3. Specification of Security Requirements** - The security requirements for the system should be stated and specified. This project specifies requirements through the list of policies that should be implemented for this scenario.
- **4. Design and Development of a Security Architecture** - A security architecture to protect the smart grid system should be designed and implemented. Taking into account the use cases and security requirements outlined in the previous steps. This project aims to design and show implementations of policies and protocols in Scyther which meet the outlined security requirements.
- **5. Assessment of implementation** - The architecture should be assessed against the defined security requirements to test if it is fit for purpose. This project will use Scyther's protocol verification tools to test the protocols against the requirements defined [14].

3.1 Threat Model

The threat model below shows some of the attack vectors and vulnerabilities an adversary could exploit within my scenario:

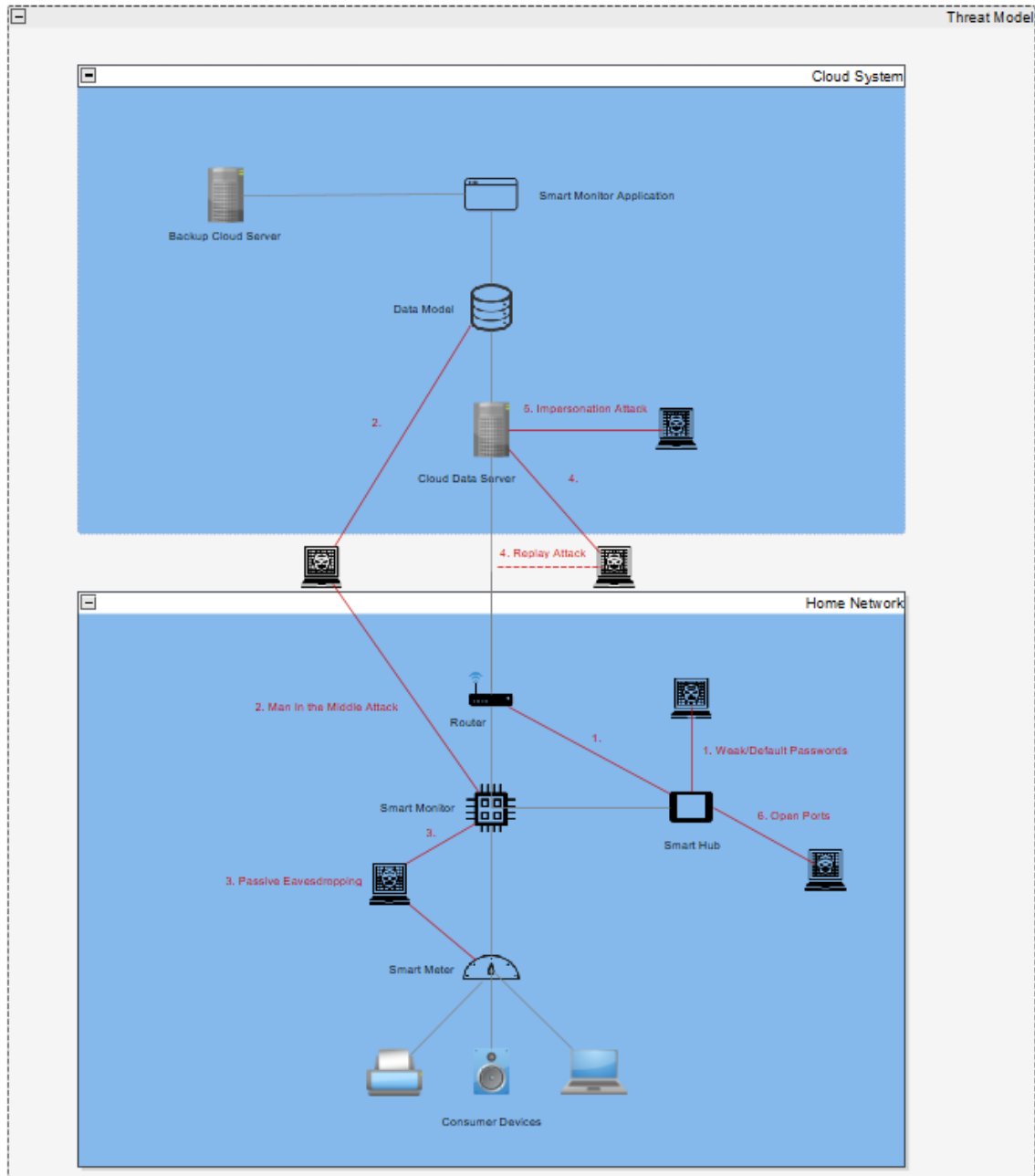


Figure 2: Threat Model of my smart grid scenario

A detailed breakdown of each threat and how they can be mitigated through the application of security protocols can be found in the preceding sections.

3.1.1 Weak/Default Password Fuzzing Attack

OWASP [15] states that the most common vulnerability exploited in IoT devices is the use of weak or default passwords. Using a list of just 60 common passwords, the Mirai botnet was able to infect and recruit over 500,000 IoT devices.

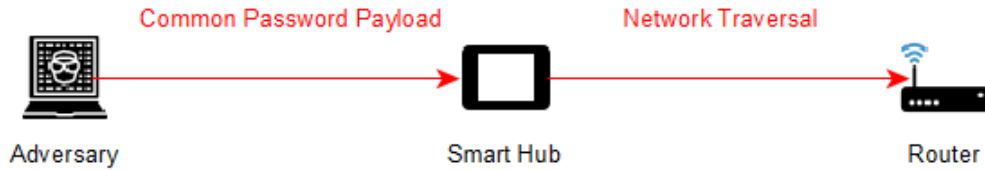


Figure 3: Adversary using a common password to compromise the network

In this scenario an adversary could exploit an internet connected smart hub with a guessable password to recruit the device into a botnet or potentially use the compromised device as an attack vector into the rest of the network.

3.1.2 Man In The Middle (MITM) Attack

Man in the middle attacks occur when an adversary is able to act as an intermediary or proxy between communication parties without their knowledge.

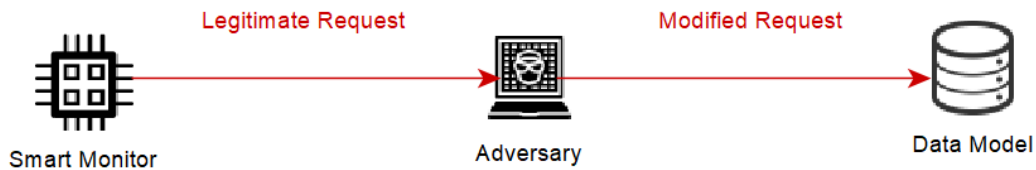


Figure 4: Adversary relaying and modifying smart monitor data

An Adversary could perform a MITM attack by secretly relaying and modifying the electricity usage information sent to the data model. A large scale attack of this kind effecting many monitor to model connections could cause false data injection attack on the smart grid system as this false data could cause the system to make an incorrect decision when routing power.

3.1.3 Passive Eavesdropping

Low power IoT devices commonly use weak or no cryptography in their communications protocols, this means an adversary could read the packets sent between devices. OWASP [15] lists these insecure protocols as the 2nd most common IoT vulnerability.



Figure 5: Adversary reading an insecure communication

This attack could occur anywhere in the scenario where devices communicate with each other insecurely. For example, the adversary could sniff packets between the smart meter and monitor to know if a home is occupied based on their current electricity usage or to gather information on the network for further attacks.

3.1.4 Replay Attack

Replay attacks occur when an adversary is able to identify and collect authentication credentials from a legitimate communication and use those credentials in a later communication to bypass authentication.

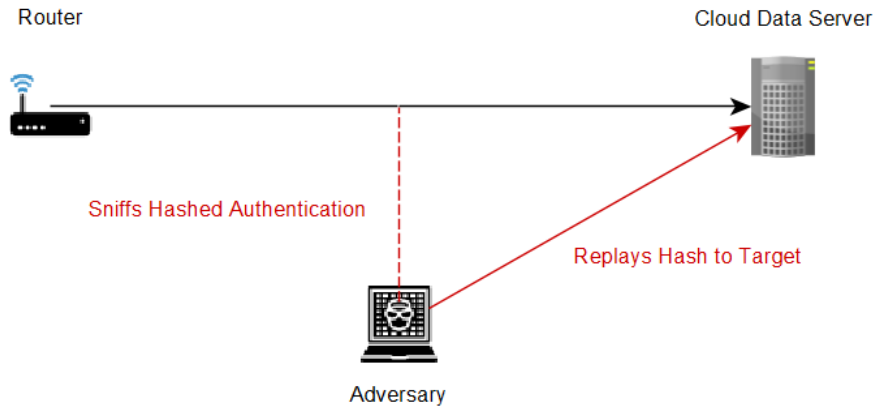


Figure 6: Adversary sniffing and reusing hashed authentication credentials

The adversary could sniff an encrypted communication between router and server used for the transmission of energy usage data. With this they could use the hashed authenticator code to send messages to the server posing as that home network without needing to know the actual authenticator code.

3.1.5 Impersonation Attack

An Impersonation attack occurs when an Adversary is able to pose as the identify of a legitimate party in a communication protocol allowing them to bypass authorisation or act on the legitimate user's behalf [16]. Protocols that do not use unique tokens for each communication are particularly susceptible to this form of attack.

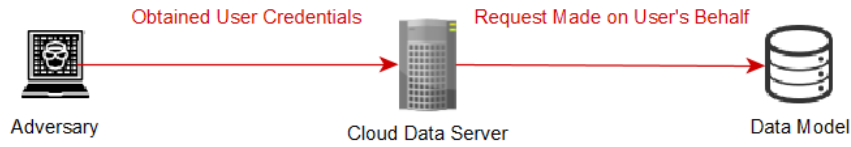


Figure 7: Adversary posing as a legitimate smart meter

An adversary could use this attack to pose as a monitor communicating data model and may use this to report false energy readings reducing trust in the system or use this access to perform further attacks against the infrastructure.

3.1.6 Open Port Scanning

An open port refers to a device accepting packets from a certain port number. If ports are not configured correctly, adversaries can use a insecure port that has not been blocked as an attack vector. Botnet recruitment malwares such as Mirai scan these ports to identify IoT devices that can be compromised. [17]

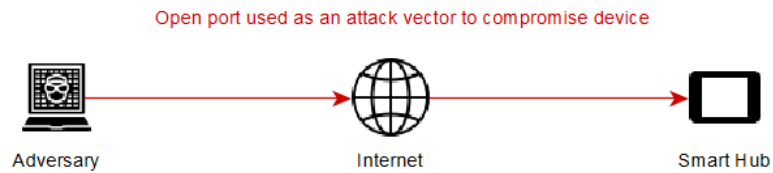


Figure 8: Adversary using an open port to attack a device

This attack can occur in the scenario where any devices are configured to allow network traffic in from unnecessary communication protocols such as telnet (port 23) and SSH (port 22).

3.2 Recommendation of policies and practices

3.2.1 Policy List

Based on the threat analysis of my scenario and my research I am recommending the following initial policies. These policies will be modelled in Scyther and the protocols that I create will be evaluated against them.

Number	Policy	Description	Reason for Inclusion
1	Suitable Password Management	1. Default passwords must be changed 2. Passwords should be a minimum of 8 characters and not feature common phrases	Will Mitigate the threat of default/weak password fuzzing attacks
2	Network Segregation	Smart Grid IoT devices should be segregated from the consumers home Wi-Fi network	Isolates system from the consumers potentially insecure home network
3	Patch Management	Security patches for devices and software in the system should be applied and tested in a timely fashion	Reduces exposure to known and patched vulnerabilities
4	Minimum design	The hardware design should include the minimum features required for operation of the hardware. Unnecessary ports should be closed	Unnecessary features and ports being enabled create additional attack vectors for adversaries
5	Communication between parties should be secure under the following sub standards		
5.1	Mutual Authentication	Mutual Authentication should be achieved by both communication parties	Increases the difficulty of an adversary posing as a communication party
5.2	Message Encryption	Information contained in communications should be encrypted	Encryption prevents an adversary sniffing information over an insecure network
5.3	Implicit key authentication	No entity other than the one specifically identified can gain access to the cryptographic key	Necessary for encryption to be robust
5.4	Unique Session Keys	Communication Parties should establish a unique session key valid for a single communication	Unique session keys prevent the re-use of authentication credentials

Table 1: The initial policies recommended for the project.

4 Implementation and specification of non-communication IoT policies

4.1 Smart Hub password management

In a study examining user behaviour toward password policies, Inglesant [18] found that excessively restrictive password policies with too much of a focus on password complexity caused users to adopt insecure workarounds such as writing down passwords or using the same password across multiple accounts. Therefore, a good password management policy should aim to balance the need for users to choose a password that is unique and complex enough to not fall victim to common password list and brute force attacks whilst also not being too restrictive or complicated that the user has to resort to insecure methods of remembering it.

Based on this, the following key points are recommended for the implementation of an effective IoT password management policy:

- Passwords must be at least 8 characters long
- Before hashing, passwords should be checked against OWASP's top 10,000 password list [19]
- Created passwords must only be used for the Smart Hub

5 Implementation and modelling of communication protocol policies

5.1 Message Encryption

The first policy to be implemented is message encryption. As this policy is designed to mitigate the threat of passive eavesdropping, I am defining the implementation successful if an adversary is unable to decrypt and read either the key or freshly generated message using a passive Eavesdropping attack.

5.1.1 Design

The design is a symmetric encryption/decryption protocol. The symmetric key design was chosen as it requires less computational power than asymmetric options and potential issues with key distribution are mitigated as communication parties remain constant therefore keys only have to be distributed once which can be in a controlled environment.

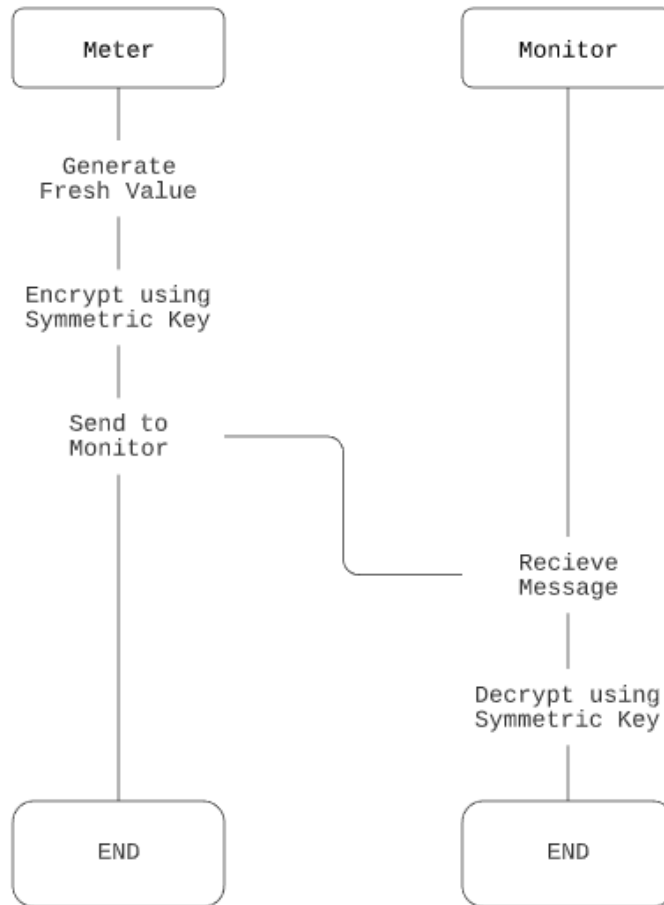


Figure 9: Message encryption protocol design

5.1.2 Implementation

The implementation of the design in Scyther is a two-way communication where the Meter sends information to the Monitor and the Monitor sends back a confirmation of having received the message.

```
1 protocol smartExchange(Meter,Monitor)
2
3   {
4
5     role Meter {
6
7       fresh Message: Nonce;
8
9       send_1(Meter,Monitor,{Message}k(k));
10      recv_2(Monitor,Meter,{Message}k(k));
11
12      claim_Meter1(Meter, Secret, Message);
13      claim_Meter2(Meter, Secret, k(k));
14
15    }
16
17    role Monitor {
18
19      fresh Confirm: Nonce;
20
21      var Message;
22
23
24      recv_1(Meter,Monitor,{Message}k(k));
25      send_2(Monitor,Meter,{Message}k(k));
26
27      claim_Monitor1(Monitor, Secret, Message);
28      claim_Monitor2(Monitor, Secret, k(k));
29
30    }
31
32 }
```

Figure 10: Message encryption protocol in Scyther

5.1.3 Review

To model the requirements of both the freshly generated value and the key not being disclosed, Scyther's Secret claim was made on the message which models an adversary attempting to eavesdrop on the message during communication.

Without the implementation of the symmetric key encryption, running the secret claim generates a successful eavesdropping attack.

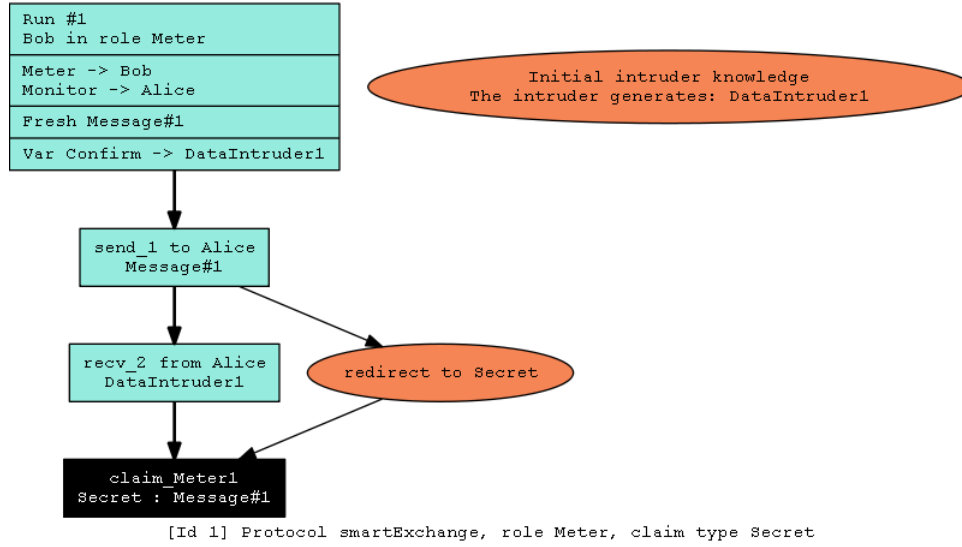


Figure 11: Message encryption protocol test results

The figure above shows by eavesdropping the message, demonstrated in this case by DataIntruder1 the adversary can read the contents of the message therefore disproving the secret claim.

The first iteration of the protocol passed these tests successfully with Scyther showing that no attacks of this type are possible within the bounds of the protocol. Results using a wider range of claims however show that threats such as man-in-the-middle attacks can easily break this protocol demonstrating the need to iterate upon it and implement the remaining policies

Claim				Status	Comments
smartExchange	Meter	smartExchange,Meter1	Secret Message	Ok	No attacks within bounds.
		smartExchange,Meter2	Secret k(k)	Ok	No attacks within bounds.
	Monitor	smartExchange,Monitor1	Secret Message	Ok	No attacks within bounds.
		smartExchange,Monitor2	Secret k(k)	Ok	No attacks within bounds.

Figure 12: Message encryption protocol test results

5.2 Unique Session Keys

5.3 Unique Session Keys

6 Plan for remaining work

When referring back to NIST's [14] guidelines for the analysis and security implementation of a smart grid system, the first 3 phases defining use cases, risk assessment and specification of security requirements are reviewed in this report. Whilst the specification of security requirements will be further developed, the main focus of my remaining work is on the design and development of a security architecture and the assessment of the implementation of this architecture. This is reflected in my Gantt chart (fig:13) which shows how I plan to break down this work into tasks and my expected timings for each of these tasks.

6.1 Risk Analysis

I have identified 5 risks as key risks which could impact on my delivery of the rest of the work. The grid below shows my plan to mitigate these risks and my assessment of any residual impact that may linger.

Risk	Baseline	Mitigation	Residual
Scyther stops being supported on modern operating systems and I lose my access to the software	Impact: 5 Likelihood: 2 Score: 10	I am using vagrant to set-up a box with Scyther and all the software required to run it installed so I always have it available, the vagrant box has a cloud backup	Impact: 5 Likelihood: 0 Score: 0
I fail to manage time correctly on the project and do not finish parts	Impact: 4 Likelihood: 3 Score: 10	My Gantt chart will help when identifying if I am falling behind schedule on certain parts. Meeting weekly with my supervisor where I share my progress will also help me hold myself accountable for work.	Impact: 4 Likelihood: 1 Score: 4
My laptop is lost, stolen, or damaged causing me to lose all the content on the hard drive	Impact: 4 Likelihood: 2 Score: 8	My project files are uploaded to Git and frequently pushed to the remote branch when I make changes. I can continue to work on my desktop and the university computers.	Impact: 3 Likelihood: 1 Score: 3
My remaining work is larger or more difficult than I anticipated meaning I fail to complete parts of it	Impact: 4 Likelihood: 3 Score: 12	My background research and experience of learning Scyther in the last month has helped me estimate the difficulty of each task.	Impact: 3 Likelihood: 2 Score: 6
Personal/family issue	Impact: 3 Likelihood: 3 Score: 9	Use the university support service when needed. Keep my supervisor informed	Impact: 2 Likelihood: 3 Score: 6

Table 2: Qualitative risk analysis and mitigation plan for the key risks

6.2 Gantt Chart

My Gantt chart details my time management plan for the progress report and future plan for the rest of the project.

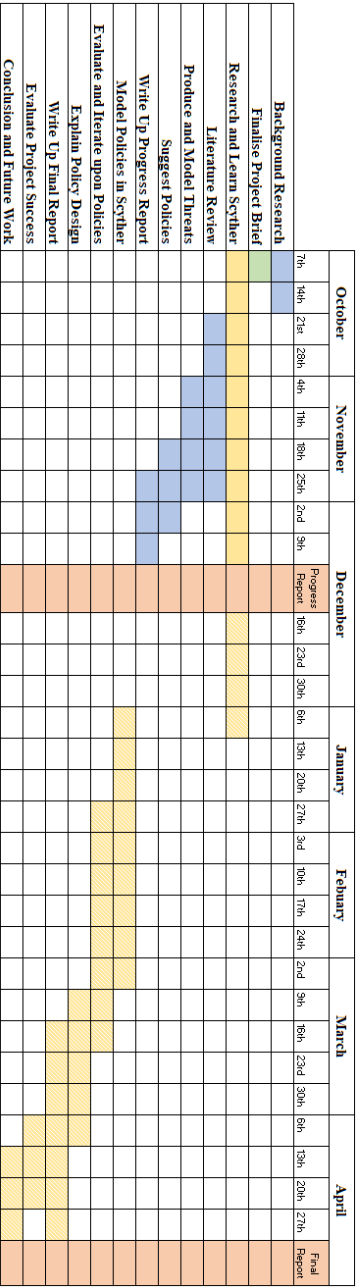


Figure 13: Gantt chart for the project

References

- [1] Keyur K Patel, Sunil M Patel, et al. Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5), 2016.
- [2] Xinghuo Yu, Carlo Cecati, Tharam Dillon, and M Godoy Simoes. The new frontier of smart grids. *IEEE Industrial Electronics Magazine*, 5(3):49–63, 2011.
- [3] Boris Kuslitskiy. Smart grid features - ansi blog, Jul 2019.
- [4] Rosslin John Robles and Min-kyu Choi. Assessment of the vulnerabilities of scada, control systems and critical infrastructure systems. *Assessment*, 2(2):27–34, 2009.
- [5] A. Sajid, H. Abbas, and K. Saleem. Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges. *IEEE Access*, 4:1375–1384, 2016.
- [6] Mercy Bere and Hippolyte Muyingi. Initial investigation of industrial control system (ics) security using artificial immune system (ais). In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, pages 79–84. IEEE, 2015.
- [7] Nikos Virvilis, Dimitris Gritzalis, and Theodoros K. Apostolopoulos. Trusted computing vs. advanced persistent threats: Can a defender win this game? *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, pages 396–403, 2013.
- [8] Leyla Bilge and Tudor Dumitras. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12*, pages 833–844, New York, NY, USA, 2012. ACM.
- [9] Yongge Wang. sscada: securing scada infrastructure communications. *arXiv preprint arXiv:1207.5434*, 2012.
- [10] Miles A McQueen, Wayne F Boyer, Mark A Flynn, and George A Beitel. Quantitative cyber risk reduction estimation methodology for a small scada control system. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, volume 9, pages 226–226. IEEE, 2006.
- [11] Cas JF Cremers. The scyther tool: Verification, falsification, and analysis of security protocols. In *International Conference on Computer Aided Verification*, pages 414–418. Springer, 2008.
- [12] Catherine A Meadows. Formal verification of cryptographic protocols: A survey. In *International Conference on the Theory and Application of Cryptology*, pages 133–150. Springer, 1994.
- [13] Nitish Dalal, Jenny Shah, Khushboo Hisaria, and Devesh Jinwala. A comparative analysis of tools for verification of security protocols. *International Journal of Communications, Network and System Sciences*, 3(10):779, 2010.
- [14] George W Arnold, David A Wollman, Gerald J FitzPatrick, Dean Prochaska, David G Holmberg, David H Su, Allen R Hefner Jr, Nada T Golmie, Tanya L Brewer, Mark Bello, et al. Nist framework and roadmap for smart grid interoperability standards, release 1.0. Technical report, 2010.
- [15] Owasp internet of things project, 2018.
- [16] Carlisle Adams. *Impersonation Attack*, pages 286–286. Springer US, Boston, MA, 2005.
- [17] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.
- [18] Philip G. Inglesant and M. Angela Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, page 383–392, New York, NY, USA, 2010. Association for Computing Machinery.
- [19] OWASP. Most common password list.