CHAPTER 1

Introduction

In a world where more and more electronic devices are connected to the internet, information security proves to be an ever important topic. It is not uncommon to see critical equipment connected to the internet, such as industrial and infrastructure equipment, medical devices [10] and even tea kettles [2]. These connected devices can be valuable targets for malicious people who seek to obtain information either for personal or professional gains. What could be gained from the devices could either be critical information that can be sold off or information that can be used to further exploit devices and systems. Such attacks have been observed many times in the past. An example is the Mirai Botnet [4], in which attackers took control of hundreds of thousands of IoT and embedded devices, and used them for Distributed Denial of Service (DDoS) attacks [3]. This type of attack is just one example of the types of attacks which could be performed by gaining unauthorized access to important systems and devices. Other types of attacks come from the most powerful organizations in the form of foreign hostile governments which impose a serious threat to other nations [6]. If hostile nations gain access to other nations systems and infrastructure, the possibilities for malicious activity are endless and could be used to exploit information and use it against other nations such as interfering in government activities. An example of hostile nation attacks can be seen from the Stuxnet computer worm attack that was discovered in 2010 [8]. Stuxnet was allegedly developed by Israel and was mainly targeting Iran's nuclear program by infecting and taking out their nuclear plants around the country. This was achieved by exploiting Siemens PLCs within the plants and altering how the machinery operated which would cause plants to stop functioning correctly. With an increasing threat of being attacked over the internet, the importance of securing critical infrastructure is more important than ever and as seen with the Stuxnet example, even smaller components have to be secured from being exploited.

To help protect oneself against such attacks the most efficient way is to properly configure the devices and networks. Properly configuring systems include keeping everything updated, configure strict firewall rules and ensure strong access control and authentication. However, even that might not be enough if an adversary has developed new, unseen attack methods that are almost impossible to counter. These are known as 0-day attacks and are some of the most dangerous attacks that can occur. In this case, the last line of defence will be a good monitoring system, which can detect

irregular behaviour in devices or systems and make operators aware of the situation to counteract the malicious attack as fast as possible. Methods such as keeping logs of commands used within the system can be used or using more advanced algorithms to predict irregular behavior within the system are key to detecting and protecting one self against malicious attacks.
One company interested in monitoring systems and devices is Telenor. Telenor is a telecommunications provider operating primarily in Scandinavia and Asia. To its customers, Telenor provides Mobile phone service, wireless and wired broadband and TV services. In 2018 Telenor served 174 million mobile phone customers[5]. Telenor operates its own infrastructure and is therefore a key provider of broadband access for its customers.
Telenor has for a long time created and managed systems of varying sizes and as such wants to protect them by becoming better at monitoring activity on them. This can come in the form of authentication monitoring and User Activity Monitoring (UAM) [9] [1]. Telenor has therefore decided to work with students at AAU to come up with a proof of concept solution for their systems. As such, Telenor has made a project proposal which will lay the foundation to help find a solution.

1.1 Project Proposal

Telenor have one or more critical systems inside its network which have been supplied by a third party supplier. These systems must be serviced by the supplier who reside in a foreign country. The service is done by remote access over the internet. A simple overview of it can be seen on fig. 1.1.

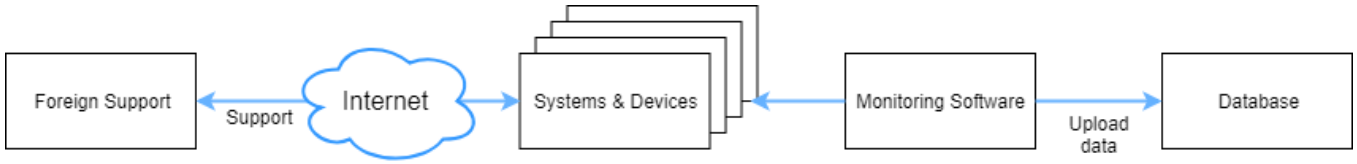

Figure 1.1: Proposed simple model of a system getting foreign support while being monitored.

For this reason, Telenor would like assistance from AAU in developing a system which can:

- Provide access management for the system and its users.
- Monitor usage of administrative commands executed on the system.
- Identify changes made whenever a technician performs remote support on the system
- Make sure the support connection originates from the correct location
- Verify the authenticity of the connected service technician.

In short, Telenor wants to find inspiration to create a better authentication, authorization and monitoring system for systems that are going to receive foreign support.