Table of contents

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. Companies are using the internet to remote control critical systems over long distances in order to improve workflow and efficiency. 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 [INSERT EXAMPLE HERE]. 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 [7]. 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 [13]. 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[4]. 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) [14] [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.

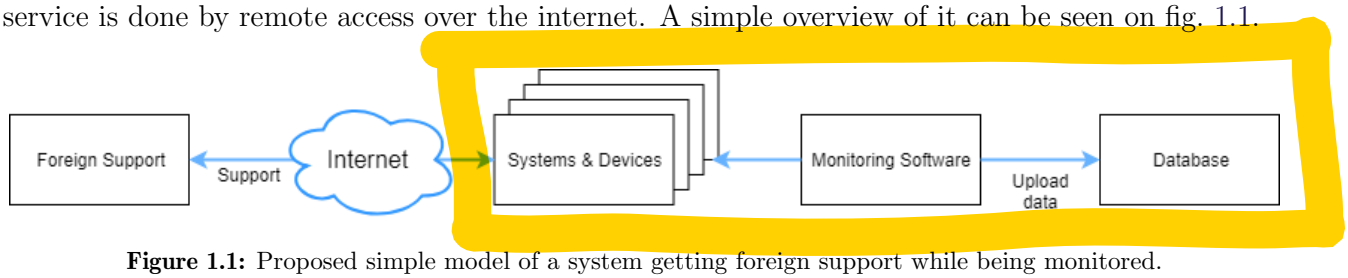

Figure 1.1: Proposed simple model of a system getting foreign support while being monitored.

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 and monitoring system for systems that receive third-party support to combat potential malicious attacks.

CHAPTER 2

Problem Analysis

To develop a technical solution in a potentially big dynamic system, it is important to fully understand the context in which the solution will operate in. Since the focus is relying heavily on the security aspect of the system, having a robust, catchall system in place to cover as many security holes as possible is needed. Furthermore, it is also needed to understand Telenor as a company and what their priorities and ideas for the system are, so the solution will have a maximum effect for the system the solution should operate on. As such, the following is taken into consideration when figuring out how the proposed system should be made based on the project proposal (section 1.1):

- Secure, verified network/system access
- Authentication of systems/users
- In-system monitoring
  - System logging
  - User Activity Monitoring (UAM)
  - Third-Party Activity Monitoring (TPAM)

The systems which needs protection and monitoring are operating inside Telenors' network, while being supported by a remote third-party company. This creates a potential security problem for Telenor, since the remote supporters must have access to Telenor's network in order to do their jobs. These types of security problems are known as insider threats where people from within the third-party company are the security liability. To avoid security problems with third-parties, making sure that their remote actions stay within company policy is needed. This, however, isn't possible by simply logging the activity and going through them after the fact. This means that more powerful measures are needed to have the capability of actively monitoring what is happening on systems receiving third-party support as well as knowing if the right person is connecting and supporting the system by proper authentication. Monitoring and acting on all actions performed by the third party is necessary in order to make sure that no insider threat occurs. By doing so, it is possible to see who did what, when and why and react in real time to the unauthorized activity. To achieve this,

some form of data is needed to classify what action within a system is valid or invalid in order to decide if the third-party support is doing what they are supposed to do or if there is potentially some malicious activity going on.

2.1 Authentication

Before a user even gets to access the system which is being monitored, it is necessary to authenticate them. Authentication is the process of verifying the true identify of a connecting user. It can also be tied to access control where different authenticated users has different access privileges, depending on their job function. The ultimate goal of an authentication system is to allow only the intended people can access the system and in turn, make it impossible for anyone else to access the system. Authentication systems can consist of multiple layers of authentication depending on the needed level of security. More layers provides more security but can potentially also make the system more frustrating to use for intended users, since they have to provide additional information to be authenticated.

2.2 Active Monitoring System

To monitor a system and being able to stop potential malicious attacks a method of active monitoring an individual system in real time is used. Doing so enables the ability to record and process activity happening on a system while a user is interacting with it in real time. Compared to the non active monitoring where you would only collect data in form of logs and process it later, the active component can actively process and stop malicious activity as it happens, making sure that an attacker wouldn't have enough time to steal or harm any data on the system. An example of this can be seen on fig. 2.1.

Figure 2.1: Proposed simple model of a system getting foreign support while being actively monitored.

As seen on fig. 2.1, the `Monitoring Software` actively monitors what is going on on the system and if the `Processor` flags something as potentially malicious, the `Monitoring Software` cuts off the connection between the user and the system. In an ideal world, the `Processor` would be able to determine if an action is malicious instantaneously as it happens, but when taking several parameters into account such as processing time and transferring data between several systems for processing, making instantaneous decisions is impossible. However, the processing could be localized to the machine where the `Monitoring Software` is running on but in that case the processing of the data would take away resources from the system which would slow it down and potentially make it unusable. As such, using external processing and data collection is required to avoid slowdowns on a system at the cost of having a delay in how fast the `Monitoring Software` can react to malicious activity. Delays are not the only aspects that impact an active monitoring system, several other

factors decide how efficient and how cost-effective the system is in reality as seen in the following section.

2.2.1 Effects of Active Monitoring

With employing an active monitoring system, several advantages and disadvantages come with it. These can be seen, depending on your use case, as a good thing or a bad thing. With Telenor, the active monitoring systems are going to be used on critical infrastructure systems rather than monitoring individual systems such as an employees computer. The critical systems could contain sensitive data and giving employees of a third-party support company access to is could create several liabilities for a company such as Telenor. Risks such as disclosure of confidential information, duplication of files, file transfers and more create the need for active monitoring to avoid any data from being stolen and potentially used against the company. The advantages for the active monitoring can be summed up as follows:

- Preventing incidents in real time before damage is done.
- Potential to recognize real vs fake employee.
- Save time and resources from security problems post incidents.
- Streamlines the investigation after the fact. If something goes wrong, you have enough data to know what happened.

As it can be seen from the list above, actively monitoring the system comes with several advantages where it all boils down to making sure that the person within the system is known and authenticated. If anything goes wrong such as an malicious action, preventive measure can made before any serious damage can be done. This results in saving time and money after the fact since proper measure have been taken to log and monitor what had exactly happened in the moment that the incident happened. But with all advantages there are also some disadvantages which are as follows:

- Third-party support have to go through more hoops to do their work.
- A company has to spend more time and money managing the monitoring systems and databases.
- Large amounts of data are generated from the monitoring software which needs to be processed.

With the disadvantages, the major aspect is time and cost of running the active monitoring system. First the third-party support would have to go through extra authentication to be able to connect to the system that they want to use. Second, the company hosting the active monitoring system would have to employ people maintaining and updating the systems and software to be up to date in regards to security and company policies.
An aggressive logging system has the danger of producing large amounts of data which are not useful. Therefore care should be taken when building such a system, as to not produce unnecessary noise since it will take up unnecessary space and make it harder to filter through the log events.

2.2.2 Classification of Malicious Activity

As seen on fig. 2.1, the proposed system can actively decide if something happening in the system is malicious or not. The question is how do you actually define what is malicious activity and what is not malicious activity? This can be achieved in several ways where one of them comes in the form of a `Classification System` where depending on several variables in different scenarios, a performed action can either be classified as good or bad.
Classification systems will inherently have some degree of imprecision. This will cause the system to entirely miss malicious actions or misclassify normal actions as malicious. This is known as false negatives and false positives. For such a system to bring value, it will need high enough precision to catch a significant amount of hostile actions (keeping false negatives to a minimum), while keeping the and false positives down to a minimum. False negatives i were the system is not able to detect malicious activity, where false positives is valid actions that is detected as malicious. Kaspersky have made a malware "classification tree" where the types of behaviour that pose the least threat are shown in the lower area of the diagram and the types of behaviour that pose a greater threat are displayed in the upper part of the diagram.[5]

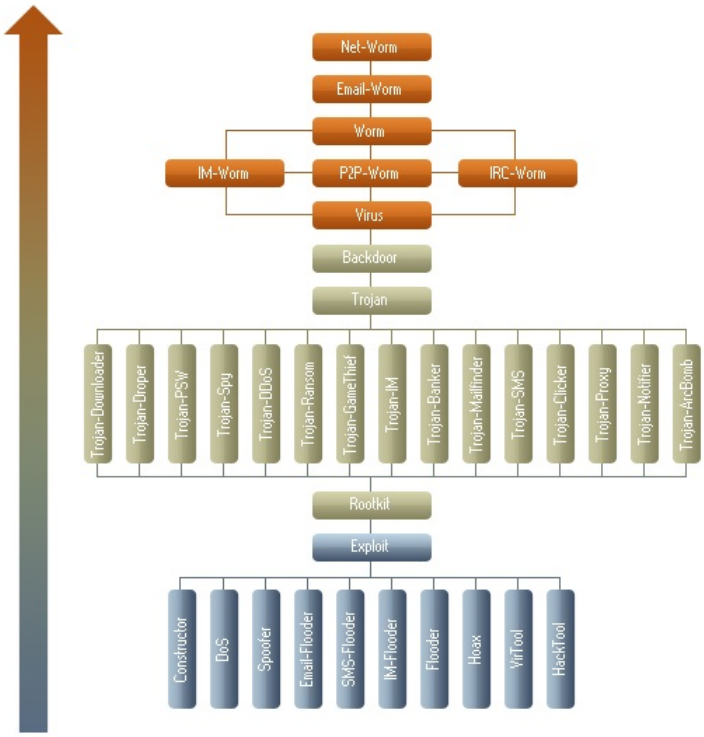

Figure 2.2: malware "classification tree"[5]

This type of classification tree can be modified to fit other threats or unwanted behaviour where the threats can form the tree be prioritized.

2.3 State of the art

To get an understand of what methods, tools and ideas are used for authentication, monitoring and governance systems, this section and the following subsections will take a look at what the current state of art is for these three topics.

2.3.1 Active Monitoring Systems

As mentioned earlier, the Active Monitoring Systems are used to make sure that whatever happens within a system is monitored and if something suspicious happens, preemptive actions must be taken to avoid serious damage to the system.
When a malicious agent successfully gets past the authentication system and gains direct access to a system, it is necessary to detect the intrusion in the system via active monitoring software. In this case, the software to detect intrusions is an Intrusion Detection System (IDS) [12].

There are two types of IDS': the ones who try to detect known malicious activity, which simply cut the connection when the criteria defining a Malicious Activity are all met, and the systems that detect malicious activity as a deviation from normal, regular behavior. For the second type of IDS, using machine learning algorithms are necessary. Although their use is not mandatory for the first kind of systems, they generally use it.
The first type is weak when it comes to new, previously unknown types of attacks, also known as zero-day attacks, but it will always detect known attacks. The second type of IDS has been trained to detect anomalies in behavior within a network, so they can detect known attacks well, but they are also more vulnerable to false positives, since deviations from regular behaviour can start alarms, even though sometimes, a non-malicious user will behave in that way.
For protecting highly sensible data, system operators usually use hybrids of both types of IDS, which have the benefits of both types. It has been proved that this approach works better than just using one of them.
As mentioned before, this type of algorithm works by using machine learning. The most widely used machine learning techniques for IDS' are Ant Colony optimization, Cuttlefish algorithms and Genetic algorithms. Datasets for training purposes are widely available where the most commonly used is the KDDCup99 Dataset [8].
The IDS can be host based or network based. In the case of an host-based intrusion detection system (HIDS), it runs on the system devices and analyzes the data on the devices themselves [10]. In the case of a Network-based Intrusion Detection System (NIDS), it analyzes traffic at a strategic location in the network, such as Ethernet packets for example [11].
The data used by those system is of different types, but the methods used to analyze them in order to detect whether there is a threat or not are the same.

There exists many types of IDS' which are used but because of its many flaws an upgrade was made called Intrusion Prevention System (IPS) in order to both detect and prevent intrusions better than the regular IDS [9]. The upgrade that an IPS offers over and IDS is that the IPS sits in front of a network instead of on top of a network like the IDS does. By doing so, the IPS can prevent attacks from even getting into the network by using packet inspection on the connection and only allowing the connection into the network if everything is in order with the data transmitted. In many cases a combination of both IDS and IPS is preferred to allow for better security before a connection is

granted access and analyzing the connection when it has been allowed into the network.

2.3.2 Authentication

These days, user and systems authentication are necessary to protect systems and data from any risk. It is common practice using user name and password as a type of authentication, but this is not enough as it's weak and easy to discover by hackers. There are some improvements to that, it is a more complicated password choice, consisting of capital and small letters, numbers and symbols. However, this is also not enough to make sure that the user is the actual user and not someone else who has the login information.

Two-factor authentication is used to increase the degree of protection. It is done by a code which can be sent to a mobile device or by a special external device that generates the code. An example of a popular code type is the Time-based One-time Password (TOTP)[6]. This type of authentication looks better than a simple password, but there are weaknesses in this way in which case the mobile phone or the code generator device does not work or is lost. In this case, the user cannot access the system.

Fingerprints is another type of two-factor authentication, which has some positive aspects for ease of use and cannot be lost like the code generator device or mobile, and through which it recognizes that the user is the actual user.

Also, there is a method of authentication which is by allowing the user to access the system if the user is in the correct geographical location and through a specified IP address or through a specific device using its MAC address.

Using machine learning as a type of authentication, and that done by making the monitoring system understands and recognizes the user's methods and behavior, for example, the system can learn the user behavior and pattern of writing messages, passwords or through the way the user usually accessing the systems' files and what time in which it is done. By learning all that, the monitoring system can distinguish between the real user of the device from unauthorized one.

In addition to authenticating users, it is also possible to authenticate the user's computer. This is done by a Trusted Platform Module (TPM)[3]. A TPM module is a special secure hardware module built into a computer, which is capable to performing cryptographic tasks. This involves memory for storing cryptographic keys and perform cryptographic hashing algorithms. The module is built to be tamper resistant, such that physically modifying the hardware is hard or impossible. A TPM is often used to unlock full an encrypted disk when the computer boots. Here the encryption system verifies that the disk is still in the correct computer and that the users storage is not under attack. A similar process can be used for remotely authenticating the computer through the process called Remote attestation, where the computer's hardware is verified.

2.3.3 Governance

When it comes to security policies, they can make a huge impact on the probability of intrusion. The best practice for companies is to have well-defined security policies, to assure confidentality,

integrity and availability for their information systems and internal networks based on the aims of company. This implies on having a security framework that considers the organisation‘s security objectives – what is considered as a risk based on service the organisation provides, etc. The security program consist of many components: risk management, risk assesment and analysis, security documentation, information classification and protection, auditing, layers of responsibility, security control implementation and management.
There are more security standards that can be followed, such as ISO/IEC 27000-series [2] or NIST Cybersecurity Framework. All of the standards have similar lifecycle:

- Plan and organise
- Implement – develop and implement security policies, procedures, baselines and guidelines
- Operate and maintain
- Monitor and evaluate

To maintain security for evolving company, the security program must be regularly revised and updated. Every policy has its boudaries – the employees must follow it in order to achieve the security. This means that one of the most important part (after implementing the standards) of the policy is the awareness training.

2.4 Solution Proposal

This section describes the technical and ideal solutions based on what requirements Telenor wanted from the project while making it fit into the project scope.

The solution to be made which is ideal for Telenor is a ”proof of concept” solution consisting of methods and ideas for a solution that Telenor can take and make themselves. Because of this, the proposed solution for this project won't be a hand over box solution for Telenor. Though this still means that the proposed solution will have the functionality of a product that can be used but will never go beyond the stages of a proof of concept solution. As such, the following sections will describe the ideal solution for the project and will go over the different aspects of the proposed solution that will be focused on.

2.4.1 Authentication

Telenor has a fixed set of remote supporters who needs access to the system being monitored. Therefore the authentication needed for the system will have to focus on allowing people from specific third party companies to access to system. That could be people from a specific physical locations or IP addresses. This means the authentication system potentially needs to be location aware. Further, the authentication system will need to authenticate individual supporters with some form of multi-factor authentication.

2.4.2 Database synchronization

Since the data generated on the critical systems needs to be processed, the data should be moved out of the system and processed on another system to reduce load on the critical system. To do so, some form of database synchronization is required between the two systems. Not only does the data need to be transferred, the `Monitoring Software` also needs updates on what is going on within the critical system at all times. This means that data needs to be sent between both systems in a bi-directional way where data is sent to be processed and the result of said processing would be returned either showing that everything is okay or something is wrong.

2.4.3 Light Weight Monitoring Software

To meet the requirement of having non-obtrusive software running, the software to be made for the proposed system, `Monitoring Software` and `Authentication` `Software`, needs to be as light as possible. The focus of the software needs to not interfere in what happens on the system, especially system critical systems that need a specific amount of resources to run. If the resources are used up by our own software, the system wouldn't potentially be able to run properly and would cause problems on a larger scale.
Having the software light weight is also one of the reasons why the proposed system is split into several parts. One of them is to be located on the system to be monitored and one on another system where the main processing of data happens. This way, system load on the critical systems would be reduced.

CHAPTER 3

Problem statement

The challenges proposed by Telenor come in the form of a pure technical solution based on the fact that the proposed solution is incorporated into already existing infrastructure where the solution will be a layer on top of it. Due to the magnitude of possibilities associated with the project, the scope of the project was needed to be delimited in order to create a product that would be functional and cover a good amount of areas for the desired solution. As such, the focus of the project and the proposed solution will focus on a small network of computers where the focus will be on monitoring and data collection to maximize the solution of creating a secure remote access monitoring system. Thus the problem statement based on the problem analysis is as follows:

"How can a system be designed to monitor and collect data from foreign connections to create a secure remote access monitoring system."