**Assignment #2: Cybersecurity in Smart Farming**

Group 02: Ahmad Malkawi, Alberto Araya Rojas, Syed Muhammad Hasan Haider, and Vineet Muthyalu

School of Information Technology, Fanshawe College

INFO-6010: CISSP Prep

James Robertson

November 22, 2024

**Introduction**

In this case study, we will be exploring a scenario related to the Agrotech industry. The problem at hand is that Tania has joined an AI based farming team called Agritech AI (ATAI) hands to help run her agriculture business with the help of AI based equipment. In this paper, we will discuss the possible threats that this new change poses and a multi-layered security strategy to help protect this agriculture infrastructure. We will also be creating an incident response plan for one security incident. This plan will ensure business continuity and disaster recovery. As per the scenario, Tania has received an anonymous tip claiming that ATAI is selling data related to her farm without her consent. We will be investigating possible ways of evaluating this claim and create a strategy for the protection of Taniya’s data, starting with a plan for improving Taniya’s cybersecurity literacy.

**Infrastructure and assets**

To analyze threats, we must know what assets and infrastructure we intend to protect. In this section, we aim to identify all the assets and explain the infrastructure of the system at hand. “An asset is, by definition, anything of worth to an organization” (Maymi & Harris, 2021, p. 213). In this case, we have tangible assets like the machinery, which includes drones for crop monitoring, autonomous tractors for plowing and planting, sensors for animal needs/activities, and robots for various tasks such as feeding animals and crops, and a central server to manage these machines using Artificial Intelligence. We also have intangible assets such as the data in transit, data at rest and data in use. “Data-in-transit refers to data actively moving from one location to another across a network or from a local storage device to cloud storage.” (Swanzy & Ansong, 2024, p. 63) In this case, it refers to the data being sent from the sensors to the central management server and the data sent from the server to the machines. “Data-at-rest is

data sitting on a computer, a server or somewhere in the cloud” (Swanzy & Ansong, 2024, p. 62a). For project scenarios, this refers to the system information, log of transit data, analysis results etc. “Data-in-use refers to data that is being processed by one or more applications and not just stored passively on a hard drive.” (Swanzy & Ansong, 2024, p. 62b). For ATAI, this is the data that is currently being analyzed by the Artificial Intelligence to give appropriate command to the autonomous machines.

As per the scenario, the infrastructure built by ATAI consists of sensors that collect data about the current situation of the crops. This data is sent to the central management server, which saves this data in its database and performs analysis on this data to give commands to the machines and autonomous robots on the field to take necessary action.

**Threats to the System**

Now, we will discuss the threats posed to this infrastructure and to the assets involved. “A threat is any potential danger that is associated with the exploitation of a vulnerability.” (Maymi & Harris, 2021, p. 8a). “A vulnerability is a weakness in a system that allows a threat source to compromise its security.” (Maymi & Harris, 2021, p. 8b) The sensors could be hacked or could malfunction and give incorrect data, which would result in a wrong analysis and a wrong action taken by the machines. The threats to these sensors could be physical, that is, someone creates an artificial environment around the sensors or tries to break them. Since the sensors do not take any input from the system (i.e, their only source of input is the data gathered from the environment), there is no data being transferred from the server to the sensors. This means that sensors are only subject to physical threats. “The main threats that physical security components combat are theft, interruptions to services, physical damage, compromised system and environment integrity, and unauthorized access.” (Maymi & Harris, 2021, p. 220).

The sensors send the data to the main server. This data in transit could be intercepted by a malicious actor, who could gather and change information being transferred. This is an example of Man in the Middle Attack “The idea behind a Man-in-the-Middle attack is intercepting communication originating from one machine and delivering it to the intended receiver without them being aware that their traffic has been read and maybe manipulated”. (Samuel & Somasundaran, 2022, p. 2) The data could also be subject to noise, making it ineffective.

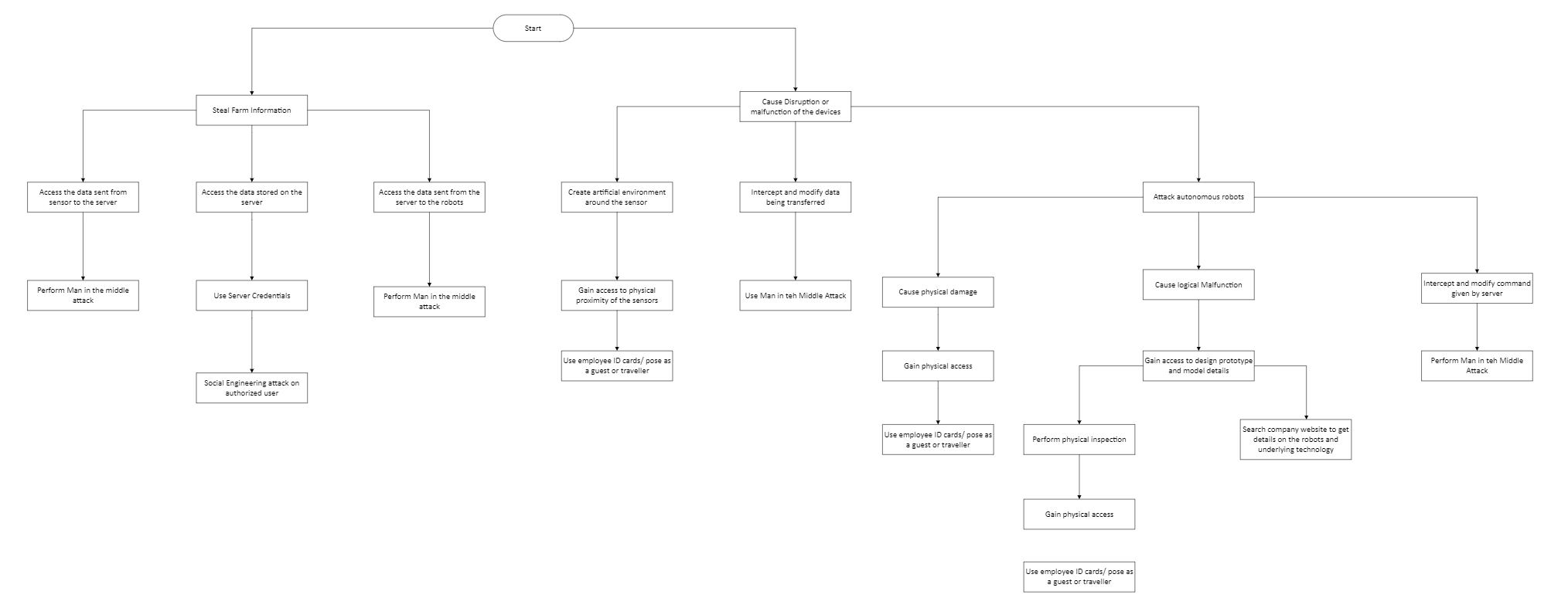
Once the data reaches the server, it is stored in a database. The server could be subject to a malicious attack where an attacker attempts to gain unauthorized access to the server and/or its resources. To do this, the attacker would try to exploit the vulnerabilities of the server, which could include both hardware and software vulnerabilities. If the server requires credentials to login, the attacker might try some social engineering attack tactic, such as a phishing attack to trick an authorized user to hand over the server credentials to the malicious threat actor. “The most common form of social engineering is phishing, which is the use of e-mail messages to perform social engineering.” (Maymi & Harris, 2021, p. 42). The attacker might try to extract the information or just gain maximum control of the server by installing a rootkit. “A common rootkit definition is a type of malware program that enables cyber criminals to gain access to and infiltrate data from machines without being detected.” (Fortinet, What Is a Rootkit? How to Defend and Stop Them?, 2024). This maximum control would allow the attacker to guide the autonomous robots as per their will. The physical location of the server is also an important factor to consider here as the attacker might just physically install malware or try to harm/destroy the server.

The data (or command) that is sent from the central server to the autonomous robots is susceptible to Man in the Middle Attack. As these communications are done via satellite, they can be intercepted by performing a satellite eavesdropping attack, “where an eavesdropping satellite can intercept optical communications established between a low Earth orbit (LEO) satellite and a high-altitude platform station (HAPS).” (Yahia, Erdoğan, & Kurt, 2021, p. 1).

Autonomous robots take server commands as input and perform actions accordingly. The threat actor could attempt to hack these robots and machines using the hardware, software or implementation vulnerabilities in their design. Just like the sensors and the server, these robots are also susceptible to physical attack.

Before diving into the strategy, we must select a framework for prioritizing the threats so that Tania and ATAI can make decisions based on their budget and the priority of threats. For this, we will start with building an attack tree. “An attack tree is a graph showing how individual actions by attackers can be chained together to achieve their goals”. (Maymi & Harris, 2021, p. 386).

The following attack tree summarizes the kinds of attacks that the user can perform and the motives that they could have behind each attack.

****

*Figure 1*

As depicted in *Figure 1* the attacker could have two motives behind the attack. Either the attacker wants to steal data from the system, or the attacker wants to disrupt or destroy the system. There could also be a combination of both motives. For stealing the information, the attacker would implement a passive attack strategy. The attacker’s goal would be to listen to the data being transferred, used or stored. For this, the attacker would use Man-in-the-Middle Attack. If the motive is to destroy/disrupt the system, the attacker would try to modify the data being transferred to ensure that the autonomous robots perform as per the attacker’s desire.

We will now use the Risk matrix to assign priority to the threats. “A risk assessment matrix, also known as a Probability and Severity or Likelihood and Impact risk matrix, is a visual tool depicting potential risks affecting a business.” (Vicente, 2024).

For this case study, a simple 3x3 risk assessment matrix will be used.

|  | **Low Impact** | **Moderate Impact** | **High Impact** |
| --- | --- | --- | --- |
| **Unlikely** |  |  | Physical modification of autonomous robots |
| **Likely** |  | Physical destruction of devices | Man in the Middle Attacks |
| **Highly Likely** |  |  | Unauthorized server access |

As per the risk assessment matrix, the physical and technical threats that had been identified can be prioritized in the following order:

1. Unauthorized server access
2. Man in the middle attacks
3. Physical destruction of devices
4. Physical modification of devices

Based on this approach, we can now work towards the creation of a security strategy that would ensure protection of the infrastructure.

**Multi-layered Security Strategy**

Since the threats are posed to multiple layers (physical, logical, technical) of the infrastructure, the security strategy has been designed to protect assets at each layer.

To prevent unauthorized server access, must ensure that all the data in use, data in transit and the data at rest is encrypted. To protect from Active Man in the Middle attack, we must ensure that Hashing is used to check for data integrity. “Hashing is a one-way mathematical function that turns data into a string of nondescript text that cannot be reversed or decoded.” (Vaideeswaran, 2024). We can also perform a network segmentation over this network so that if one part is compromised, the rest of the network remains secure. “Network segmentation is an architecture that divides a network into smaller sections or subnets. Each network segment acts as its own network, which provides security teams with increased control over the traffic that flows into their systems.” (Fortinet, What is Network Segmentation?, 2024). We can deploy a honey-pot to catch any attacker trying to access our network. “A honey pot is a security resource whose value lies in being probed, attacked, or compromised.” (Jammi, Raju, & Munishankaraiah, 2010, p. 1). This would help to detect an intruder and could set the security to high alert. We must backup all the data regularly on a separate physical storage that is not part of the network.

To prevent anyone from physically destroying autonomous robots or sensors, physical security measures such as a physical security team and AI-enabled CCTV monitoring system that also serves as a physical Intrusion Detection System must be implemented. Relevant personnel could be given authorization to access areas where they can perform their jobs. Role Based Access Control can be implemented to ensure that no one has access to any resources or areas that are not relevant to their jobs. This restricted access would also prevent anyone from physically modifying the devices.

**Incident response plan**

Despite all the security, a breach is always possible. In this section, we will discuss how we can respond to such security incidents and mitigate the risks while ensuring business continuity. For this case, we have chosen to discuss how to respond if someone manages to gain unauthorized access to the server, encrypts all the data, and is now demanding a ransom of 30 bitcoins to release the data. No one is able to access any data and they can all only see a prompt demanding the ransom.

To tackle this, we must be clear about the two kinds of risks. First is the risk that can be mitigated, and the impact can be minimized. Second is the residual risk, which is the risk that remains even after all the mitigation.

The first step of the plan is getting compromised components off the network. For this, all the network components that were breached to allow this escalation of privileges need to be identified, starting with the access layer of the network, which contains user computers. Look at the network logs for any anomaly in user network traffic including shady downloads or unusual requests for granting access to other resources. After this, the attack pattern must be tracked to identify all the components that were breached. We must use spare/backup resources to replace these devices. This would ensure that there are no known compromised components remaining in the network. Then, we will use the backup server and provide it with the latest backup data that was stored on a physical device separate from the network. This would allow it to get our network up and running with minimal downtime and minimal data loss. However, the residual risk remains that the attacker might have taken a copy of the data before encrypting it. This means that the data confidentiality is compromised, and it can be leaked or sold to adversaries. This is a risk that can not be mitigated and must be accepted.

**Tania’s technical literacy plan**

As a major stakeholder in this system, Tania must have at least the fundamental technical knowledge of cybersecurity. In this section, we will propose a practical plan to improve Tania’s awareness.

Taniya must start with an introduction to a cybersecurity awareness workshop. Tania should attend such workshops since they provide fundamental knowledge on how users of the internet can keep themselves safe from cyber-attacks.

Tania should join a cybersecurity training group where she learns basic access control mechanisms and can identify the security flaws that can be seen in plain sight. These include physical security and logical access control.

It is important to realize that Tania does not have a technical background, and she might not have enough time to get a career level (or professional) cybersecurity training. Tania must transfer security risk to someone else. Any company that offers cybersecurity insurance could be selected for this purpose. This team of professionals would not only analyze the security posture of the farm but also educate Taniya on the security risks and how to handle them.

**Investigation for Data Skimming**

As per the anonymous tip, ATAI might be skimming money or stealing data from her. The safest approach is to hire a third party that would perform complete security and financial auditing of ATAI. For the security audit, the team would analyze the overall security posture of ATAI and check their databases for any data that has been transferred to unusual places. The financial audit would help her understand the flow of money and if she is being taken advantage of. It is important to note that since the initial contract has already been signed, ATAI might not be very cooperative to allow such audits since it would disrupt their operations and challenge their reputation in the market. For this purpose, Tania would require legal support. Another approach can be to check for the current auditing firms that have been auditing ATAI. Financial audits are legally mandatory in most countries and companies can not do business without that. Gathering this data and getting help from accountants can help her make sense. As a stakeholder and owner of the farm, Tania does have every right to challenge ATAI on its policies and, therefore, take away her business from the company if they do not agree to her terms. She could ask for a new contract that mandates financial and security auditing by a mutually agreed upon third party to remove any biases in the future.

**Reflection and Conclusion**

This assignment has challenged us to critically evaluate our knowledge by working in a team and by solving a real world problem. Working as a team came as a blessing to us, since we all got to see every member’s skills and abilities. We also learned how to navigate a work condition where task delegation has to be done in the earlier stages of the project. We all managed to use our knowledge from the contents of CISSP CBK, which was our primary source of reference, as well as the knowledge that we gained from other courses in the program. This task was a good comprehension of the concepts learned throughout the program. We managed to reevaluate the way we looked at security issues and gained an interesting perspective on how to implement security controls while considering the fact that the end users and stakeholders might not be security professionals themselves.We learned how to manage an Agrotech project from a security perspective and how to investigate and respond to security incidents. We also learned the significance of regular auditing (especially during a merger or an acquisition). We learned how to develop a plan to increase awareness of stakeholders regarding cybersecurity so that they can conduct business in a safe environment.

# **References**

· Fortinet. (2024, November 15). What is a rootkit? How to defend and stop them? Retrieved November 15, 2024, from<https://www.fortinet.com/resources/cyberglossary/rootkit>

· Fortinet. (2024, November 15). What is network segmentation? Retrieved November 15, 2024, from<https://www.fortinet.com/resources/cyberglossary/network-segmentation>

· Jammi, A., Raju, Y., & Munishankaraiah, S. (2010). Intrusion detection through honey pots. International Journal of Engineering Science and Technology, 2(12), 1. Retrieved from<https://www.researchgate.net/publication/50361771_INTRUSION_DETECTION_THROUGH_HONEY_POTS>

· Maymi, F., & Harris, S. (2021). CISSP all-in-one exam guide (9th ed.). McGraw Hill LLC.

· Samuel, B., & Somasundaran, V. T. (2022). Prevention of man-in-the-middle attacks using blockchain VPN. Current Journal of Applied Science and Technology, 6(12), 45. Retrieved from<https://www.researchgate.net/publication/366303575_Prevention_of_Man-in-the-Middle_Attacks_using_Blockchain_VPN>

· Swanzy, P. N., & Ansong, E. D. (2024). Data security framework for protecting data in transit and data at rest in the cloud. Current Journal of Applied Science and Technology, 43(6), 61–77. Retrieved from<https://www.researchgate.net/publication/380543798_Data_Security_Framework_for_Protecting_Data_in_Transit_and_Data_at_Rest_in_the_Cloud>

· Vaideeswaran, N. (2024, February 6). Hashing in cybersecurity. Retrieved from CrowdStrike:<https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-hashing/?srsltid=AfmBOopuxYEexmNBMjntHuzYFyL07yKRTzHuQ58oC6RA-HYsC4Er1ilL>

· Vicente, V. (2024, February 15). *Risk Assessment Matrix: Overview and Guide*. AuditBoard. Retrieved November 15, 2024, from

<https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/>

· Yahia, O. B., Erdoğan, E., & Kurt, G. K. (2021). Optical Satellite Eavesdropping. *Research Gate*, *1*(1), 1. <https://www.researchgate.net/publication/356904298_Optical_Satellite_Eavesdropping>