CYBR 271 Secure Programming (2024)

Student ID: 300655437

Student Name: Sahil Adwani

a. Persona Non Grata Exercise

PERSONA #1:

Name: James Field
Demographics: CIS male, 45 years old
Background: James is a maintenance technician with 15 years of experience in vending machine repair. He holds a background in mechanical engineering and practical expertise in machine maintenance. After being fired from the company that produces the vending machines due to a minor infraction, James became angry and dissatisfied. His therefore, struggles led him to sell his grandad's truck and therefore he wanted revenge upon the company.

Primary Goal: Revenge on the company by causing their business to go down.
Specific Objectives:

- Sabotage vending machines physically to cause operational disruptions, causing frustration for users and hence financial losses for the company.
- Leak sensitive information and data about the company to the public and social media to damage its reputation and weaken customer trust.

Skills:

- Expert in mechanical and electrical repair, disassemble and modification skills specific to vending machines from previous experience.
- Knowledge of vending machine systems and operational weaknesses in vending machine designs from engineering background.

Resources:

- Tools and equipment for repairs (can be used for sabotage)
- Still holds access to company systems, data and internal knowledge
- Industry contacts to spread information or cause disruptions.

PERSONA #2

Name: Emily Carter
Demographics: CIS female, 28 years old
Background: Emily has a degree in Cybersecurity and has accumulated 6 years of experience as a cybersecurity analyst. Recently, she left her job to start her own cybersecurity consultancy. However, she has struggled to attract clients and generate sufficient income.

Primary Goal: Achieve financial gain through malicious activities targeting vending machines.
Specific Objectives:

- Carry out a man-in-the-middle (MitM) attack to secretly intercept and manipulate the data being sent between the vending machine and the company's central systems
- Steal money or redirect funds
- Create fake transactions to gain money unlawfully
- Sell or exploit sensitive information.

Skills:

- Expertise in cybersecurity, including experience with network attacks/security, data manipulation, transaction security vulnerabilities and MitM techniques from previous experience.

Resources:

- Access to advanced hacking tools and software for conducting MitM attacks (packer sniffers and traffic analysis tools).
- Connections with other cybersecurity professionals or hackers

PERSONA #3

Name: Alex Rivera

Demographics: CIS male, 21 years old
Background: Alex is a self-taught cybersecurity enthusiast with a strong interest in activism. He became passionate about cybersecurity through online communities and has honed his skills by participating in various ethical hacking forums and workshops. Alex harbours a deep-seated dislike for Coca-Cola due to the company's environmental practices, which he believes are harmful to sustainability efforts.

Primary Goal: Force the vending machine company to stop selling Coca-Cola products.

Specific Objectives:

- Launch a Distributed Denial of Service (DDoS) attack on the vending machines to disrupt their operations causing inconvenient for users and the company.
- Continue the attacks until the vending machine company agrees to stop selling Coca-Cola products.
- Use the disruptions as a platform to draw attention to his protest against Coca-Cola, leveraging media coverage and public attention to address his environmental concerns.

Skills:

- Expert in cybersecurity, network vulnerabilities, network attacks, particularly DDoS attacks and ethical hacking.
- Experience in digital activism, including organizing online protests.

Resources:

- Access to DDoS attack tools and techniques.
- Connections with other activists or hacker groups who share similar goals.
- Utilization of media and social media platforms

b. Misuse Exercise

MISUSE CASE 1:

Preparation:

James gathers tools and equipment, including specialized devices from his time as a technician (screwdrivers, circuit testers and wire cutters)

He identifies vending machines owned by the company through his insider knowledge and selects locations with high traffic to maximize impact

Gaining Access:

Using his knowledge of the machine's design, James approaches the vending machine during off-peak hours when the locations are less crowded

He leverages his experience to bypass basic security measures like locks and alarms, gaining access to the internal components of the machines.

Sabotage Actions:

James disconnects and damages critical components such as motors, dispensing mechanisms and card reader. This prevents the machine from functioning correctly.

He also alters the wiring which could also cause hazards like minor electrical fires or shocks.

Lastly, James would extract the information about the vulnerabilities and methods he used for sabotage and leak this information to the public and social media, disclosing private information.

Consequences:

The machine experience frequent breakdowns, leading to customers frustrated and lost sales.

Company is forced to spend extra resources on repair and maintenance.

Company faces with increased negative reviews hence harming the company's reputation.

Persona Link:

James's background as a maintenance technician gives him the skills and knowledge to execute this misuse case effectively. His motivation for revenge is directly tied to his former employment, driving his desire to cause harm to the company through physical sabotage.

MISUSE CASE 2:

Preparation:

Emily investigates to find the communication protocol used by the vending machines. She gathers information on the encryption methods, payment processors and network infrastructure used by the company

She sets up a secure remote server to which can route intercepted data, configure hacking tools like packet sniffer and traffic analyser to monitor the network traffic between the machine and company's central servers.

Network Infiltration:

Emily gains access to the network either by exploiting an unsecured Wi-Fi connection used by the vending machines or by compromising a network router in close proximity.

She deploys her MitM tools to intercept the data packets being exchanged between the vending machines and the payment processing system. This gives her real-time access to sensitive information, including credit card details and transaction data.

Data Manipulation:
Transaction Interception: Emily modifies the transaction data in real-time, redirecting funds from customer purchases to accounts she controls. This is done by altering the payment destination while keeping the transaction appearing normal to both the user and the vending machine.
Creating Fake Transactions: She inserts additional, fraudulent transactions into the network, making it appear as though legitimate purchases are being made.
Data Harvesting: Emily collects sensitive information such as credit card numbers and user credentials. This data can be sold on the dark web or used in further attacks.

Consequences:
The vending machine company faces financial losses due to the redirected funds and fraudulent transactions. Customers may experience unauthorized charges on their accounts, leading to complaints and potential legal actions. The company's reputation suffers, especially if the breach becomes public, undermining customer trust in their payment systems.

Perona Link
Emily's cybersecurity expertise, particularly in MitM attacks, allows her to exploit the vending machine's network vulnerabilities for financial gain. Her motivation stems from her financial struggles and the need to sustain her consultancy business, pushing her towards illegal activities.

MISUSE CASE 3:
Preparation:
Alex conducts online research to identify potential vulnerabilities in the vending machines' network infrastructure, focusing on how the machines connect to the company's servers.
He collaborates with other like-minded activists or hacker groups, pooling resources and coordinating the attack to maximize impact.

Launching the Attack:
DDoS Attack Execution: Alex and his collaborators use botnets or hijacked devices to flood the vending machine network with overwhelming amounts of traffic. This excessive traffic slows down or completely stops the communication between the vending machines and the central systems.
Targeted Disruption: They target specific machines in high-traffic areas and continue over time, ensuring that the disruptions are noticed by many customers. The goal is to create widespread inconvenience, leading to customer frustration and negative publicity.

Amplifying the Message:
Alex uses media and social media platforms to publicise the disruptions caused by the DDoS attack. He frames the attack as a protest against Coca-Cola's environmental practices, drawing attention to his cause and explains the motivation behind the attack.

Consequences:
The vending machines experience significant downtime, leading to lost revenue and customer dissatisfaction.
The company faces increased scrutiny from the public and media, particularly regarding their choice to sell Coca-Cola products.

Perona Link:
Alex’s self-taught cybersecurity skills and passion for environmental activism drive him to use a DDoS attack as a form of protest. His dislike for Coca-Cola and his commitment to sustainability are key motivators behind this misuse case.

c. Security Card Exercise

STORY #1
Data Breach through Employee Manipulation

1. Human Impact - **Personal data card:** The attack compromises the personal data of vending machine users, leading to potential identity theft.
2. Motivations - **Self-promotion card:** The adversary seeks recognition within a hacking community by breaching a secure system and stealing customer data.
3. Resources - **Inside knowledge card:** The attacker is an employee with detailed knowledge of the vending machine's network and data storage practices.
4. Methods- **Indirect attack card:** The adversary uses social engineering to manipulate another employee into granting access to the vending machine's backend system. Once access is gained, they extract customer data, including payment information, and publish it online, leading to widespread identity theft and reputational damage to the vending machine operator.

Story:
An ambitious IT technician working for a vending machine company is eager to prove their skills in the hacking community. They decide to exploit their access to the company’s network but lack the necessary permissions to access sensitive customer data. The technician cleverly manipulates a colleague, convincing them to share login credentials for routine maintenance. With this access, the technician extracts payment information and user data from the vending machine’s backend system. They upload this data to an underground hacking forum, gaining instant recognition and praise from peers. However, the breach causes severe harm to customers, who become victims of identity theft. The vending machine company faces lawsuits and serious damage to its reputation, all because of the actions of an insider looking to gain attention and recognition.

STORY #2
Financial Exploitation via Skimming Devices

1. Human Impact - **Financial well-being card:** The attack directly affects the financial well-being of vending machine users by stealing their payment information.
2. Motivations - **Money card:** The adversary is motivated by financial gain, seeking to profit by stealing and selling credit card information.
3. Resources – **Inside capabilities card**: The attacker is an insider with access to the vending machine, giving them the ability to install skimming devices without being detected.
4. Methods - **Multi-phase attack card:** The adversary installs skimming devices on the vending machine card readers, waits for enough transactions to be recorded, then retrieves the

devices to access the stolen data. They use the obtained data to create fraudulent transactions, impacting the financial security of users.

Story:
An employee working for a vending machine company decides to make extra money by exploiting their access to the machines. They secretly install skimming devices on several vending machines in high-traffic areas. Over the course of a few weeks, the devices collect credit card information from hundreds of customers. The employee retrieves the skimmers and sells the stolen data to criminals who use it to make unauthorized purchases. Customers begin noticing suspicious charges on their accounts, leading to widespread financial loss and frustration. The vending machine company faces backlash as customers lose trust in the security of their payment systems.

STORY #3
Physical Sabotage to Harm Competitor

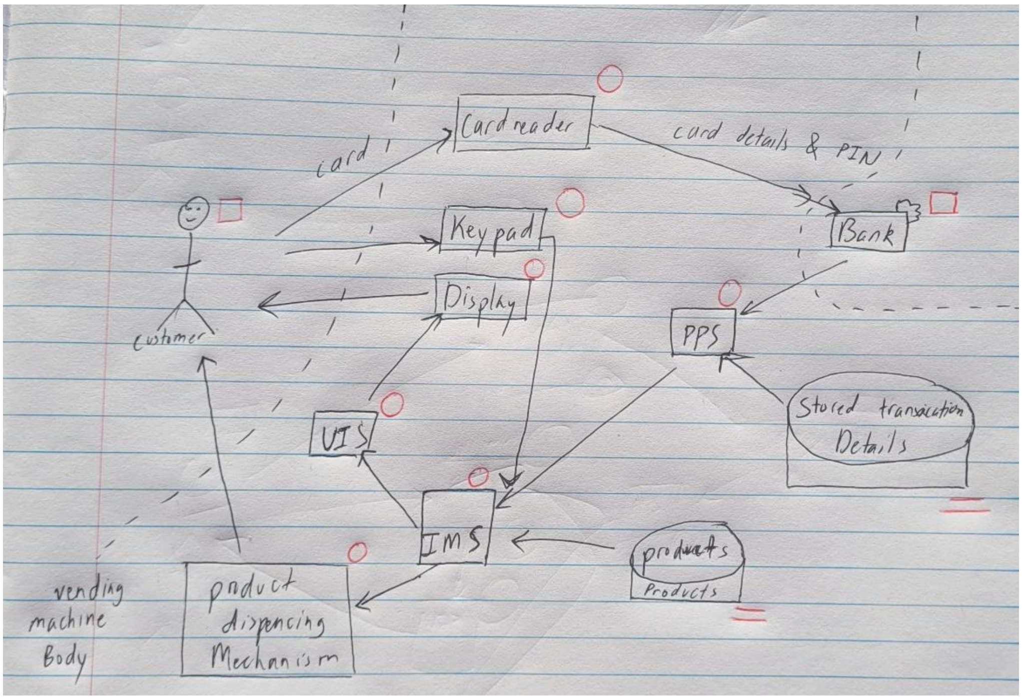
1. Human Impact **- Physical well-being card:** The sabotage results in physical harm to users, potentially causing injuries when they attempt to use the vending machine.
2. Motivations - **Malice or revenge card:** The adversary is motivated by a desire to harm a competing business by damaging its reputation through unsafe vending machines.
3. Resources - **Tools card:** The adversary uses specialized tools to tamper with the internal mechanisms of the vending machine, causing it to malfunction.
4. Methods - **Physical attack card**: The adversary physically damages the vending machine's dispensing mechanism, making it unsafe to use. When customers attempt to purchase items, the machine malfunctions, causing injuries and leading to a decline in trust and usage.

Story:
A small business owner, frustrated by the success of a competing company, decides to sabotage the competitor’s vending machines to harm their reputation. Late at night, they break into a few locations and use specialized tools to damage the internal mechanisms of the machines. The next day, customers trying to buy snacks from the machines are met with violent jerks and even electric shocks as the machines malfunction. A few customers are injured, and the incidents quickly make the news. The competitor faces lawsuits and loses customers, who now view their vending machines as dangerous. The sabotage successfully tarnishes the competitor’s image, giving the saboteur an edge in the market.

d. STRIDE Exercise

DFD DIAGRAM

NOTE:
PPS = Payment Processing System
IMS = Inventory Management System
UIS = User Interface Software
User Interface = Keypad + Display



STRIDE ANALYSIS

SPOOFING	
COMPONENT	THREAT
Customer - Interactor	**Description**: Spoofing identity of a legitimate customer **Example**: The attacker obtains personal information of a customer, such as their credit card number and user credentials, through a data breach. Using this information, the attacker accesses the vending machine system as if they were the legitimate customer using a cloned card. Vending machine doesn't verify if the customer is legitimate or a fraud. **Impact:** The attacker can make unauthorized purchases, potentially leading to financial loss for the actual customer and misuse of the customer's payment information Additionally, the customer may feel disappointed and betrayed by the vending machine company for failing to secure their payment information properly. This breach can also damage the company's reputation and erode customer trust.
Card reader - Process	**Description:** Spoofing the card reader **Example:** An attacker installs a device that mimics the functionality of a legitimate card reader onto a vending machine. This fake card reader captures the payment information, such as credit card details, as customers make their purchases. The captured data is then used to make unauthorized transactions or sold on the black market. **Impact:** Customers' credit card information is compromised, leading to financial losses and potential identity theft. The vending machine

	company faces reputational damage, potential legal consequences, and financial costs related to addressing the security breach and compensating affected customers. Attacker can used customers information to sell or use and hence gains money

TAMPERING	
COMPONENT	THREAT
Card Details + PIN from Card Reader to Bank – Data flow	**Description:** Tampering with the data flow between the card reader and the bank being card details and PIN **Example:** An attacker sets up a Man-in-the-Middle (MitM) attack by exploiting a vulnerability in the vending machine's network communication. When a customer taps their card and enters their PIN, the attacker intercepts the data as it is transmitted from the card reader to the bank's payment processing system. The attacker could modify the transaction details, such as changing the amount being charged, changing destination or capture the card details and PIN for later fraudulent use. **Impact:** The compromised data flow can result in unauthorized transactions, leading to financial losses for customers and potentially significant chargebacks for the vending machine operator. Stolen card details and PINs can be used in further fraudulent activities, exposing customers to identity theft and financial fraud. Additionally, the integrity of the payment system is severely compromised, leading to a loss of trust from customers, payment processors, and banks.
Products (Drinks and Snacks) – Data store	**Description:** Tampering with the physical products inside the vending machine, such as drinks and snacks. **Example:** An attacker gains unauthorized access to the vending machine, possibly by picking the lock. Once inside, the attacker tampers with the products by injecting harmful substances into drinks or altering the packaging of snacks to make them appear untouched but unsafe for consumption. Attacker then closes the machine, leaving the products looking normal. **Impact:** Customers who purchase and consume the tampered products could suffer from serious health issues, leading to potential lawsuits and severe damage to the operator's reputation. The vending machine might also be subject to regulatory scrutiny and mandatory inspections, leading to operational downtime and financial losses. Public trust in the safety of vending machine products could diminish, impacting the entire vending industry.

Card Reader - Process	**Description:** Tampering with the User Interface System (UIS) **Example**: An attacker gains physical access to the vending machine and changes the UIS software. They might modify the display to show fake product options or prices or redirect customers to a counterfeit payment screen. For example, when a customer selects a product and tries to pay, the tampered UIS could show incorrect prices or capture payment details through a fake payment processor controlled by the attacker. **Impact:** Customers might face issues like wrong product selections or incorrect charges. This can lead to unauthorized charges on their payment methods, causing financial loss and potential identity theft. The vending machine company could suffer financial losses and damage to its reputation. Additionally, the company may face legal troubles for not securing the UIS properly.

REPUDIATION	
COMPONENT	THREAT
Stored transaction Details – Data store	**Description**: Repudiation of stored transaction details **Example**: An attacker uses the vending machine's card reader to make a purchase, and the transaction is saved in the system. Later, the attacker claims they didn't make the purchase or that it was unauthorized. If the system's logs are not detailed or secure, it's hard to prove the transaction was legitimate. Attackers may go into the stored transactions details and hide their ones. **Impact**: The company may face financial losses from chargebacks or refunds, as they might have to cover the costs. It can also make it difficult to keep accurate financial records, manage disputes, and maintain trust with payment processors. Frequent disputes and challenges in proving transactions can undermine the effectiveness of the transaction recording system.
User Interface - Process	**Description**: Repudiation of user actions through the user interface (keypad and display) **Example**: An attacker selects a product using the vending machines keypad and confirms it on the display. Later, they deny making the selection or entering the code, claiming it was a malfunction or that someone else used the machine. If the system doesn't have detailed logs or audit trails of user interactions, it's hard to prove the attacker's involvement. **Impact**: This can lead to disputes over transactions, causing financial losses from refunds or chargebacks. The vending machine operator might struggle with reconciling user actions with system records, affecting operational efficiency and customer trust. Difficulty in resolving disputes increases customer service costs and can harm the machine's reputation, potentially leading to decreased usage.

INFORMATION DISCLOSURE	
COMPONENT	THREAT
Stored transaction details – Data store	**Description:** Information disclosure through stored transaction details **Example:** An attacker breaches the vending machine’s data storage system and retrieves detailed records of transactions, including customer credit card information and purchase history. This could be done through exploiting vulnerabilities in the database security, such as weak access controls or insufficient encryption of stored data. **Impact:** The attacker can use the stolen information for fraud, such as unauthorized transactions or identity theft. This results in financial losses for customers, damages the vending machine operator’s reputation, and could lead to legal trouble for not protecting data properly. It also decreases customer trust in the security of the vending machine’s payment system.
Inventory management system - Process	**Description:** Unauthorized access to sensitive information processed by the inventory management system. **Example:** An attacker gains unauthorized access to the inventory management system and retrieves detailed information about inventory levels, product types, and stock movements. This could be accomplished by exploiting vulnerabilities in the system's access controls, such as weak authentication mechanisms or insufficient authorization checks. **Impact:** The attacker can use the disclosed information to manipulate inventory levels, identify high-value products for theft, or gain insights into the business’s stock management practices. This can lead to financial losses due to theft or inventory mismanagement, operational disruptions, and potential damage to the business’s competitive position. Additionally, it may result in customer dissatisfaction if stock levels are inaccurately reported or managed.
Customer to Card reader (card) - Data flow	**Description:** Information disclosure from customer to card reader. **Example:** An attacker uses social engineering to deceive a customer into revealing their credit card details and PIN. For instance, the attacker might pose as company representative or technical support and convince the customer to enter their card information and PIN into a seemingly legitimate card reader. The attacker then observes the data being entered or captures it through a hidden device. This could involve standing close to the customer and viewing the information on the card reader or using a hidden camera. **Impact:** The attacker can use the stolen credit card details and PIN for unauthorized transactions, leading to financial losses for the customer and potential identity theft. The vending machine operator might suffer reputational damage and face financial repercussions from fraud and chargebacks. Additionally, the incident could undermine customer trust in the security of the vending machine’s payment system, affecting its overall reliability and usage.

DENIAL-OF-SERVICE	
COMPONENT	THREAT
User interface software - Process	**Description**: A Denial of Service (DoS) attack on the user interface software **Example**: An attacker floods the vending machines UI with excessive input requests or malicious data, causing the display or keypad to become unresponsive. This might involve sending a large volume of fake interactions or exploiting vulnerabilities in the UI software. As a result, customers cannot select products or complete transactions, as the machine's interface is either frozen or malfunctioning. **Impact**: The attack prevents customers from using the vending machine, leading to lost sales and frustration. As keypad doesn't work nor the display. The inability to process transactions impacts customer satisfaction and can harm the company's reputation. Recovery from such an attack might involve costly repairs or updates to the UI software.
Stored transaction details – Data store	**Description:** A Denial of Service (DoS) attack targets the stored transaction details **Example**: An attacker floods the database with a large volume of fake requests or corrupt data. This overload prevents the system from processing legitimate transactions or accessing transaction records, disrupting the ability to manage and review transaction details. **Impact**: The attack blocks access to transaction records, making it difficult to process transactions, handle refunds, or resolve customer disputes. This can lead to financial losses, operational disruptions, and a loss of customer trust. Additionally, the vending machine operator may face reputational damage and incur high costs for system recovery and enhanced security measures.
Customer to Card reader (card) – Data flow	**Description:** A Denial of Service (DoS) attack targets the data flow (card)between the customer and the card reader **Example:** An attacker could pay individuals to go to the vending machine repeatedly just to act, causing a queue or congestion around the card reader. This artificial line delays legitimate customers from accessing the card reader, as the device becomes overwhelmed with a high volume of transaction attempts. Alternatively, the attacker might overload the card reader's communication channels with too many signals or malicious data, preventing it from processing transactions correctly. **Impact:** The attack can lead to significant customer frustration and inconvenience, as legitimate transactions are delayed or blocked. This can result in lost sales for the vending machine operator, damage to the machine's reputation, and potential financial losses. Additionally, the operator might face operational disruptions if the attack significantly impacts the machine's ability to process transactions efficiently.

ELEVATION OF PRIVILEGE-	
COMPONENT	THREAT
Payment processing system - Process	**Threat: Elevation of Privilege in Payment Processing System** **Description:** Elevation of privilege in the payment processing system **Example**: An attacker starts with basic access to the payment system but finds a way to upgrade their permissions to an administrator level via social engineering and convinces his higher up to give him privileges . With these higher privileges, Attacker can change transaction data, view sensitive payment information, or alter system settings like payment limits. **Impact**: The attacker could perform fraudulent transactions, access confidential data, or disrupt the payment system. This leads to financial losses, damaged system integrity, and a loss of customer trust. It can also result in regulatory issues if sensitive information is exposed or if security breaches occur.

d. Risk Analysis

THREATS	D	R	E	A	D	Total	Rating
MitM attack	9/10	6/10	6/10	8/10	4/10	33/50	High
Physical sabotage	7/10	5/10	8/10	5/10	7/10	32/50	High
Spoofing	7/10	5/10	6/10	7/10	5/10	30/50	High

WHAT WAS THE PROCESS USED TO ARRIVE AT THESE SCORES?

MitM attack:

Assuming vending machine and central systems have vulnerability (unencrypted data transfer or weak network security)

9/10 for damage as it has high financial impact and data breach risks. 6/10 for reproducibility because requires need expertise in network vulnerabilities. 6/10 for the next because depends on network security vulnerabilities and need tools and software. Affected user is 8/10 as users who use vending machine will get affected specifically high traffic. Discoverabilities low 4/10 because it’s hard to identity without thorough network monitoring.

Physical Sabotage:

Assuming no cameras nearby and damage is mainly interior.

Due to vending being unsafe, customer could get electrical shocks and tap the card reader with their card, but no product comes out leading to steal of money hence 7/10. Reproducibility is 5/10 because you only need tools to physical alter the wire or damage the vending machine and but need to go different vending machines each time and in quite time e.g. night. 8/10 for just needing tools. 5/10 for affected users because some people might realise that the vending machine is not working correctly/damage hence not go near it. 7/10 for discoverability because you possibly tell that there is something wrong with the machine

Spoofing (card reader):
Assuming, only one card reader was spoofed, lack of physical security and no camera in location. Can be severe as can lead to financial consequences for both customer or company but depend on customer traffic hence 7/10. Installing a fake card reader requires skill and expertise hence 5/10. 6/10 as there are devices which can be spoofed for card readers. 7/10 depends on how many people affected but still would affect in high traffic. 5/10 might take some time before fake card reader is noticed if well disguised.

Highest risk threat is MitM attack of 34/50.

MITIGATIONS – PREVENTATIVE, DETECTIVE AND RESPONSIVE CONTROLS

THREAT	PREVENTATIVE	DETECTIVE	RESPONSIVE
MitM attack	**Encrypt Data Transfers**	**Network Traffic Monitoring**	**Incident Response Plan**

Preventive Control: Encrypt Data Transfers

Implementing end-to-end encryption for data transfers between vending machines and central systems is essential. Using protocols like TLS (Transport Layer Security), encryption ensures that data transmitted across networks remains secure and unreadable to unauthorized parties. This measure prevents attackers from intercepting and manipulating the data, thereby maintaining both data confidentiality and integrity. It is important to encrypt all communication channels and keep encryption protocols updated to counter new threats (f5,2024).

Detective Control: Network Traffic Monitoring

Deploying network traffic monitoring tools and anomaly detection systems helps identify unusual activities that might signal a MitM attack (Wikipedia. 2024). These systems continuously analyse network traffic to detect suspicious patterns or unauthorized access attempts. Early detection is crucial, as it allows for prompt action to mitigate potential damage. Implementing intrusion detection and prevention systems (IDS/IPS) and regularly updating detection rules are key to effectively monitoring and addressing new attack vectors (Kirvan, Paul. 2024).

Responsive Control: Incident Response Plan

Establishing a comprehensive incident response plan is vital for managing MitM attacks. This plan should include procedures for responding to and mitigating the attack's impact, as well as conducting forensic analysis to understand the scope and methods used. A structured response helps contain the attack, reducing overall damage. Forensic analysis provides insights into how the attack occurred, improving future prevention and response strategies. Regular testing of the incident response plan and staff training on recognizing and handling such attacks are essential for effective management (Kirvan, Paul. 2024).

COST OF PREVENTIVE MITIGATION – MitM attack
Cost of Preventative Mitigation: Encrypting Data Transfers

To determine whether the cost of implementing encryption for data transfers outweighs the potential losses from a Man-in-the-Middle (MitM) attack, I estimated the cost of the preventative measure and compared it with potential losses.

Estimating the Cost of Encryption

Initial Setup Costs (US dollars):

- Software and Licensing: Depending on the size of the organization and the scope of encryption needed, the cost of encryption software and licenses can vary. For example, enterprise-grade TLS solutions might cost around $40 to $5400 (SSL2BUY. 2024).
- Hardware Costs: If additional hardware such as secure servers or hardware security modules (HSMs) is required, costs can range from $1000 to $20000, depending on the specifications and scale. (Schlyter, Jakob. 2024) (Westburry, Christopher. 2017).

Implementation Costs:

- Training: Training staff on new encryption protocols and systems could cost approximately $1,000 to $3,000 (Markovic, Isidora. 2024).

Maintenance Costs:

- Ongoing Licensing Fees: Some encryption solutions involve annual licensing fees, which can range from $8 to $1800 per year (SSL2BUY. 2024).
- Regular Updates and Monitoring: Keeping encryption protocols up-to-date and monitoring their effectiveness might require additional resources which might be an extra $1000 just in case. This is an assumption.

Total Estimated Costs:
Setup: $2040 to $28400
Yearly afterwards: $8 to $1800 (annual maintenance
additional $1000 for updates if needed.

Potential Losses from a MitM Attack

Financial Losses:

- Customer Data Theft: Data breaches can lead to significant financial losses due to fraud and legal consequences. According to the IBM Cost of a Data Breach Report 2024, the average cost of a data breach is about $4.88 million (IBM, 2024).
- Compensation and Legal Costs: Costs associated with compensating affected customers and legal expenses can add millions to the overall loss.

Reputational Damage:

- Loss of Business: A significant breach can lead to a loss of customer trust and business. Companies often experience decreased revenue following high-profile breaches.
- Regulatory Fines: Non-compliance with data protection regulations can result in fines. For instance, GDPR fines can be up to €20 million or 4% of annual global turnover. https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
-

Operational Costs:

- Incident Response and Recovery: Costs for incident response and recovery efforts can also be substantial. This might include hiring forensic experts and repairing systems.

CONCLUSION:
Given that the cost of implementing encryption ranges from $8 to $1800 and setup fee from $2040 and $ 28400 and the potential losses from a MitM attack can be as high as $4.88 million, the cost of the preventative mitigation (encryption) is **significantly lower** than the potential losses.

The cost of implementing encryption for data transfers is relatively small compared to the potential financial, reputational, and operational losses that a MitM attack can cause. Therefore, the investment in encryption is justified as it can substantially reduce the risk and impact of such attacks.

e. Reflection

Persona Non Grata Combined with Misuse Case

Creativity:

- This approach is quite creative as it combines human-centric analysis (Persona Non Grata) with specific misuse scenarios. It encourages thinking about who might want to sabotage the vending machines and how they might exploit the system.
- By envisioning the intentions and actions of potential attackers, it helps identify less obvious threats and vulnerabilities.

Ease of Use:

- It can be somewhat complex to implement as it requires detailed understanding of potential attackers' motivations and methods. Creating detailed misuse cases requires time and effort to imagine all possible harmful actions.
- It might be less straightforward to use this approach without a clear framework or guidance on combining personas and misuse scenarios effectively.

Repeatability:

- This approach is moderately repeatable but requires significant adaptation for different contexts or systems. The creative aspect means that each application might yield unique insights, but it also means that the approach may need to be tailored to each new scenario or system.

  From Mike Potts (Potts, Mike. 2015)
- Creating detailed personas and understanding their motivations and methods can indeed provide a deeper perspective on potential threats. By thinking from the adversary's viewpoint, I can anticipate their tactics and identify vulnerabilities more effectively. This approach can significantly enhance threat modelling and the development of targeted security measures.

Security Cards

Creativity:

- Security Cards offer a structured way to identify threats by using predefined categories or questions, which can spark creative thinking. They encourage systematic exploration of security aspects by focusing on specific areas like confidentiality, integrity, and availability.
- The creativity comes from how the questions or prompts are applied to the specific context of the vending machines.

Ease of Use:

- This approach is relatively easy to use because it provides a clear, structured method for threat identification. The use of cards simplifies the process of brainstorming and documenting threats.
- However, the effectiveness of Security Cards depends on the quality and relevance of the questions or categories used.

Repeatability:

- Security Cards are highly repeatable because they use a standardized set of prompts or categories. They can be applied consistently across different systems or scenarios, making them useful for repeated assessments or comparisons.

  from Wind River Software, I learnt security cards develop a security mindset and really help in brainstorming and creativity. Its last working backwords and choosing the motives, resources and other factors first (Windriver. 2024).

STRIDE

Creativity:

- STRIDE is a systematic approach that categorizes threats into Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. It may be less creative in that it follows a defined framework, but it ensures that all major threat categories are considered.
- Creativity can still be applied within each category to tailor the threats to the specific system being analysed.

Ease of Use:

- STRIDE is relatively easy to use because it provides a structured method for analysing threats. The framework helps ensure that no major threat categories are overlooked.
- Its structured nature makes it straightforward to apply, but it requires a good understanding of each category to effectively identify threats.

Repeatability:

- STRIDE is highly repeatable due to its structured and comprehensive approach. It can be used consistently across different systems and scenarios, making it a reliable method for threat analysis.

Comparison

- **Creativity:** Persona Non Grata combined with Misuse Case is the most creative, as it requires imagining detailed attacker scenarios. Security Cards provide some creativity through structured prompts, while STRIDE is the least creative but ensures thorough coverage of threat categories.

- **Ease of Use:** STRIDE and Security Cards are easier to use due to their structured approaches. Persona Non Grata combined with Misuse Case is more complex and requires more effort to implement effectively.
- **Repeatability:** STRIDE and Security Cards are highly repeatable, with STRIDE being particularly useful for consistent threat analysis across different systems. Persona Non Grata combined with Misuse Case is less repeatable due to its highly contextual and imaginative nature.

  Stride really helped in identity each and every aspect of the threat down to the detail and how threat modelling can reduce attack surface. I did research from infosec (Patrick Mallory) and he said that it reduces complexity, lowers risk exposure, increase visibility and collaboration (Mallory, Patrick. 2020).

Did **research** to calculate the cost of the preventative mitigations and assess whether the cost of mitigations outweighs the potential losses. I wasn’t surprised, as realistically, there wouldn’t be much point in implementing security measures if their costs were higher than the potential losses. But I was surprised that data breaches involve so much money (4.88 million IBM) and also could give companies fine.

Reference List:

(f5. 2024) https://www.f5.com/glossary/ssl-tls-encryptionhttps://www.f5.com/glossary/ssl-tls-encryption
(Wikipedia. 2024) https://en.wikipedia.org/wiki/Anomaly_detection
(Samson, Ron. 2023) https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/
(Kirvan, Paul. 2024) https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan#:~:text=Incident%20response%20plans%20help%20reduce,the%20event%20of%20an%20incident.
(SSL2BUY. 2024) https://www.ssl2buy.com/ssl-certificate-cost
(Schlyter, Jakob. 2024) https://internetstiftelsen.se/docs/hsm-20090529.pdf
(Westburry, Christopher. 2017) https://www.quora.com/How-much-do-hardware-security-modules-HSMs-cost
(Markovic, Isidora. 2024)https://www.edume.com/blog/cost-of-training-a-new-employee
(IBM, 2024) https://www.ibm.com/reports/data-breach
(Potts, Mike. 2015) https://www.linkedin.com/pulse/know-your-enemy-motivations-methods-insider-threat-mike-potts
(Windriver. 2024) https://www.windriver.com/solutions/learning/threat-modeling#:~:text=Security%20Cards&text=Its%20purpose%20is%20to%20facilitate,than%20a%20structured%20modeling%20approach.
(Mallory, Patrick. 2020)https://www.infosecinstitute.com/resources/management-compliance-auditing/6-benefits-of-cyber-threat-modeling/