CYBR 271 Secure Programming (2024)

Threat Modelling a Modern Vending Machine

Student Name: Kamal Hafiz

a. Persona Non Grata Exercise

PERSONA #1

Who is this person?

Name: Ivan Morozov

Demographics: 32 years old, Cyber criminal

Background: Ivan is a black hat hacker who operates on the dark web. Hacking is his full-time profession and has a history of successfully stealing money from various payment processing systems.

What are their goals?

Primary Goal: To make money because hacking is his full time job.

Specific Objectives: Hack into the payment processing system, and capture credit card information from users.

What are their skills and resources?

Skills: Knowledge of hacking payment gateway systems from previous successful experiences.

Resources: Has access to a lot of illegal, high powered tools from the dark web.

PERSONA #2

Who is this person?

Name: Karen Miller

Demographics: 31 years old, female, vending machine maintenance worker.

Background: Karen recently had been declined a request for a salary raise. She now feels unfairly treated and resentment towards her employer. She knows everything about how the vending machines hardware and software works.

What are their goals?

Primary Goal: Her goal is to seek revenge from her employer and cause reputational and financial damage.

Specific Objectives: Her objective is to disrupt the inventory and physical components and possibly even steal money from the machines.

What are their skills and resources?

Skills: In depth knowledge of the vending machines hardware systems. and also the companies security measures for the hardware components.

Resources: Still friendly with her former clients who are not yet aware she is no longer an employee to maintain the vending machine. It won't be suspicious if she is hanging around exploring the machine.

PERSONA #3

Who is this person?

Name: John

Demographics: 25 years old, male, unemployed

Background: After the recent elections, he had been made redundant from his job and is struggling to find another job. He is frustrated with himself and is struggling to cope as he has a close family member who is diagnosed with a terminal illness which forces him to spend a lot of time at the hospital looking after them.

What are their goals?

Primary Goal: He feels the need to provide hospitality and food to his extended family as they are visiting from other cities.

Specific Objectives: Try to get as much food out of the fending machine without being caught.

What are their skills and resources?

Skills: Being previously employed as a penetration tester, he knows how to find vulnerabilities and break through systems.

Resources: free public Wi-Fi, experience in hacking, he also has a lot of time as he is there most of the day and night.

b. Misuse Exercise

PERSONA #1

Misuse case – Attacker uses Man-in-the-middle attack to steal credit card information.

1. The attacker scouts various vending machines to find ones with weak or outdated security protocols that make them vulnerable.
2. Attacker infiltrates the payment processing system using phishing techniques, malware and social engineering.
3. Attacker sets up a man-in-the-middle attack by intercepting credit card the data flow between the vending machine and the payment gateway. This allows the attacker to capture sensitive information such as their credit card information from users who have recently purchased a product from the vending machine.
4. Attacker notes down the credit card information and manipulates transaction logs by either redirecting funds to his accounts or by inflating transaction to steal larger amounts of money.
5. Attacker erases transaction logs and uses dark web tools to hide their activities, making it extremely difficult for investigators to trace the attack back to the attacker.

PERSONA #2 (employee physical tamper with dispensing mechanism)

Misuse case – Attacker uses insider information to tamper physical components of machine.

1. Attacker is an employee who is working as a maintenance worker and is frustrated after being declined a salary raise. The attacker is thinking about reducing profits for the company and steal money and items from the vending machine as a form of revenge.
2. To make it not suspicious, the attacker shows up in their uniform with malicious intent, uses their key to open the main door and physically tamper hardware components such as the product dispensing mechanism and sensors so that users aren't able to get their products dispensed.
3. While the attacker has access to inside the vending machine, they also steal physical cash and products as they could also look to make personal profits whilst they have accesses.

PERSONA #3 (spoofing attack)

Misuse case – Attacker carries out a spoofing attack to get free items dispensed.

1. The attacker is a visitor who is in the hotel lobby late at night, who then connects to the public WIFI available for visitors.
2. The attacker uses technical skills to carry out a spoofing attack where they impersonate a previous users payment authorization to exploit the vending machines payment system.
3. By spoofing the previous transaction on the vending machine, the attacker is able to trick the machine to dispense items without paying.

c. Security Card Exercise

STORY #1

Human Impact – Financial Wellbeing card – System has a direct impact on peoples financial assets. If an attacker hacked into the payment gateway, they could get access to peoples online bank credentials. This will have negative consequences on the user as they would incur a loss of funds and possibly even lose trust in the payment system. There is also a risk of the compromised credit card credentials being passed on to other attackers.

Motivations – Money card – Adversary could abuse the payment gateway system to steal online bank credentials from users. Any individual who has the knowledge about hacking payment gateway systems and is wanting to make personal financial gain. This may further incentivize attacks on larger systems with more financial gains for the attackers.

Resources – Tools card – Adversary could have access to various specialised tools as they may have access to them or find out about them through the dark web. Examples of these tools could include malware, encryption-breaking software and more. With an increasing number of cyber criminals, new tools are always being created and so with new tools coming out, the adversary can keep trying to hack the system until they get in.

Methods – Technological Attack card – Adversary could attack the payment gateway system which where they would be able to eavesdrop on confidential exchanges, where in this case the system is exchanging the users bank account credentials to the payment system. This can be carried out using a Man-in-the-Middle attack. This would enable an attack on confidentiality as the attack is retrieving confidential information about users bank accounts.

STORY #2

Human Impact – Physical Wellbeing card – Adversary may have been concerned with the amount of unhealthy items being sold in the vending machines and the impact this would have on peoples physical health. The adversary believes that by attacking the vending machine, they would protect users from unhealthy items in the vending machine. The adversary may have issues relating to diabetes or know someone closely related with the issue, this could have contributed to their concern.

Motivations – Malice or Revenge card – Adversary may want to tamper with the vending machines and make them unusable so that users aren't able to get their items as the vending machines broken. This would result in a financial loss for the company and a loss for users who were needing an item from the vending machine.

Resources – Inside Knowledge Card – The Adversary is an employee who has insider knowledge of vulnerabilities in the systems, maintenance patterns and other valuable information. This could allow the adversary to execute their attack more efficiently as they are more aware of the system and how it works which allows them to attack all the known vulnerabilities and even possibly attack during a maintenance check.

Methods – Physical Attack card – The adversary could gain access during a schedule maintenance check by disguising themselves as a maintenance worker and tamper with the physical components of the vending machine. The physical components they would likely target is the spiral racks and the delivery chute as these are part of the product dispensing mechanism. This would enable their attack on the availability of the system as tampering would result in the items from the machine being unable to be dispensed.

STORY #3

Human Impact – Emotional Wellbeing card – The system has an indirect impact on the emotional wellbeing of users of a vending machine. If people are stressed or tired, they may look to get a caffeinated drink from the vending machine to give them more energy and motivation. System unavailability may cause harm because users may not be able to get their caffeinated drinks which would make them tired and stressed. This is particularly important if the vending machine are placed in environments such as universities or workplaces where the users could be under a lot of workload. This wouldn't necessarily harm users but it could affect their emotional wellbeing by increasing stress.

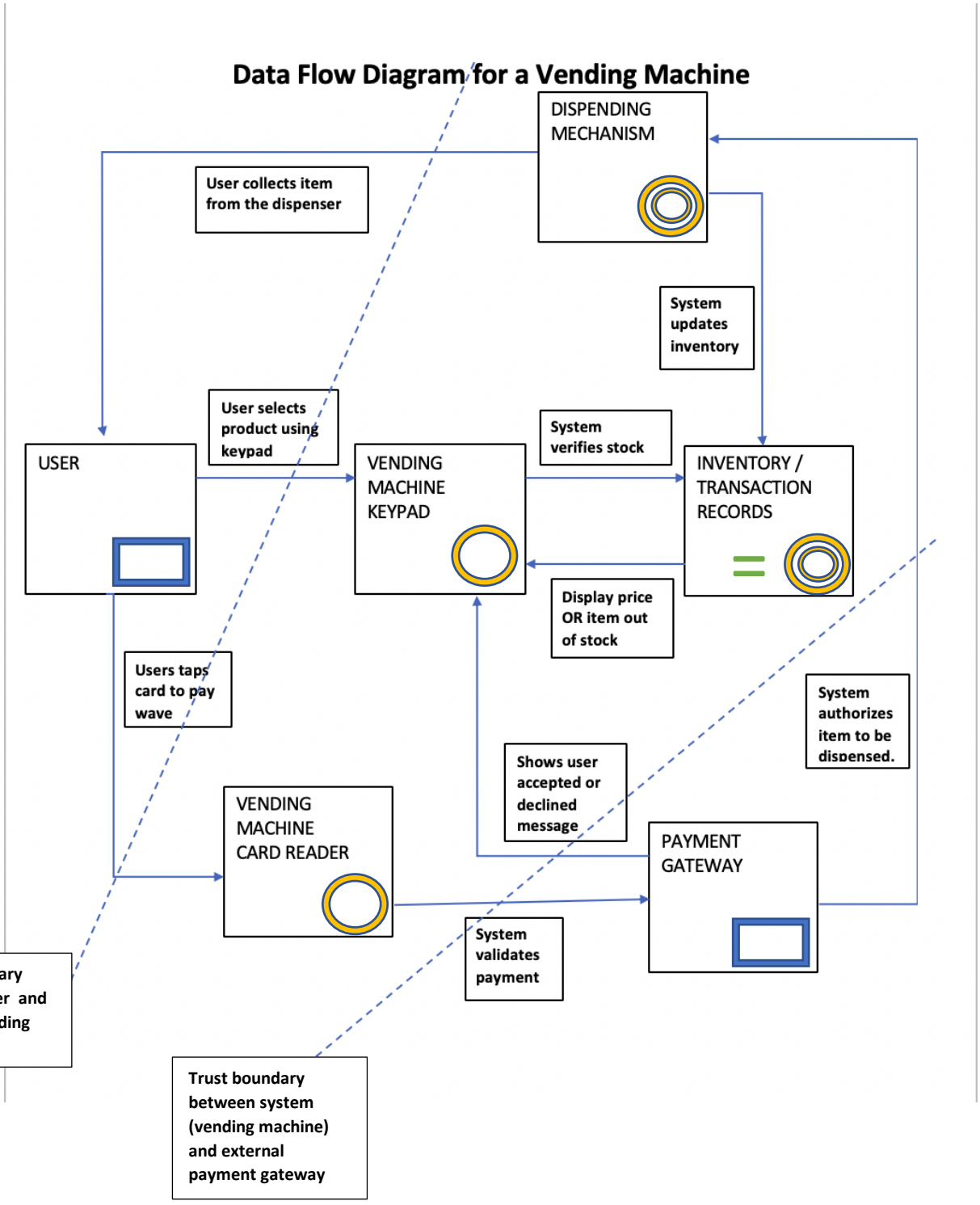
Motivations – Curiosity or Boredom card – The adversary may abuse the system by tampering with the system to obtain free items from the vending machine. An individual who has no money or has spare time and is a student at a university studying cybersecurity who is learning about offensive and defensive security methods where they learn how to execute various types of attacks. These types of students may be looking to target a vending machine system out of curiosity or as a means to practice their skills in a real life context.

Resources – Time card – the adversary could be someone who has no time constraints for their attacks. This allows them to carry out more attacks as they have time to spare, they could use trial and error to discover vulnerabilities and obtain free items from the vending machine.

Methods – Multi-Phase Attack card – The adversary uses multiple attack phases on multiple vending machines. If there are multiple vending machines in one location, they could start by testing one machine before moving onto the various other machines in the location. By testing they would try all of their skills both in the physical components and the software components to find vulnerabilities. This would amplify the attack on the availability of the system because if multiple vending machines fail, it would mean that there is less people buying items which would reduce profits for the company.

d. STRIDE Exercise

DFD DIAGRAM



STRIDE ANALYSIS

SPOOFING	
COMPONENT	THREAT
System authorization for dispensing items (data flow)	An attacker could trick the vending machine system into believing a payment was successful when it wasn't. The attacker could use a fake payment response tool to send false payment confirmation signals to get unauthorized dispensing of products as shown by the data flow from the payment gateway to the product dispensing mechanism in the DFD.
User (interactor)	An attacker could impersonate the identity of a customer to make fraudulent payments using stolen credentials. Using the stolen credit card information, the attacker purchases an item as shown by the user providing a dataflow to the vending machine reader on the DFD and causes financial loss to the rightful owner of the credit card.
User and system admin (trust boundary)	An attacker could impersonate the system's admin, obtaining access to inventory records making the system believe an item is sold out when it isn't. This is shown on the DFD diagram by the trust boundary line between the user and the internal vending machine systems. This would lead to customers not getting their product.

TAMPERING	
COMPONENT	THREAT
Dispensing mechanism(multi-process)	Attacker could alter dispensing mechanism to release products without payment verification. On the DFD diagram, this risk could occur at the dispensing mechanism multi-process component. By making the machine malfunction and drop items without payment. For example physically with the hand block or pushing against and tampering with the dispensing door to make it think it has not dropped the item yet.
Payment gateway (interactor)	Attacker could inject malware into the payment gateway interactor. This would cause the payments to redirect into the attackers bank account instead of the vending machines account. This would result in a loss for the company's profits as well as recording incorrect inventory stock.

REPUDIATION	
COMPONENT	THREAT
Vending Machine Card Reader (process)	An attacker uses another users bank card to carry out a transaction to the vending machine and then tries to deny their participation in it, saying that their account was used without authorization.
Inventory / Transaction	An Attacker could attempt to delete inventory logs to make machine think that it has run out of an item so it cannot dispense it. This would affect the availability of the items.

Records (data store)	

INFORMATION DISCLOSURE	
COMPONENT	THREAT
Card reader (Process)	Sensitive and private information such as credit card details could be exposed to attackers. If the card reader is compromised, the attacker is able to steal credit card details from users who use the vending machine. This is shown on the DFD diagram where the system uses data obtained from the card reader to make the payment using an external gateway. This shows at this process, confidential data is being collected. The impact of this would be on the company of the vending machine as they would be considered unsafe + untrustworthy after this compromise, the loss of trust would cause a reputational damage, impacting revenue and future clients.

DENIAL-OF-SERVICE	
COMPONENT	THREAT
Inventory / Transactional Records (Multi-Process / Data store)	An attacker could make the inventory records unavailable. By performing a denial of service attack, the attacker could overwhelm system to prevent it from verifying stock levels. This would make the machine unusable as users would keep getting an error message from the inventory records to the keypad saying product is unavailable as shown in the DFD.
Payment gateway (interactor)	The payment gateway system could be overwhelmed, making it non-functional. If an attacker floods the payment gateway with requests, it could cause the whole system to crash. This would result in payments being unable to be processed and the system never validates payment to dispense the product as shown on the DFD and the user receives a declined message.

ELEVATION OF PRIVILEGE-	
COMPONENT	THREAT
Payment Gateway (interactor)	The attacker could escalate their privilege by getting admin access to the payment gateway and modify transaction details. The trust boundary shown on the DFD between the user and the vending machine demonstrates this idea that the user is not within the systems administrative trust. But by bypassing this boundary, this would allow them to see the amount the user paid and redirect payments into the attacks account. This would result in a loss for the company that runs the vending machine as all their profits are being stolen.

d. Risk Analysis

THREATS	D	R	E	A	D	Total	Rating
Employee physically tampers with dispensing mechanism (Persona / misuse case 2)	3	1	3	10	10	27	High
Attacker steals credit card information through payment gateway(Security cards story 1)	10	1	3	10	1	25	High
Denial of Service attack on the Inventory / Transactional Records (STRIDE case)	4	2	3	10	3	22	Medium

WHAT WAS THE PROCESS USED TO ARRIVE AT THESE SCORES?

Employee physically tampers with dispensing mechanism

- **Damage potential (3)** The damage potential if the dispensing mechanism is physically tampered with is quite low as it would only result in one component being damaged and no harm occurring to users or financially.
- **Reproducibility (1)** The Reproducibility of this threat is low as not many employees that have access to a key would have malicious intent.
- **Exploitability (3)** The exploitability of this threat is relatively low as they would require a secure key that is only access by maintenance workers.
- **Affected users (10)** All users would be affected as they wouldn't get their items dispensed.
- **Discoverability (10)** The discoverability of this threat is quite high as any user would be able to notice a key is required to access the main door of the vending machine.

The overall risk score of this threat is 27 which is quite high, as it needs to be resolved soon as any employee with malicious intent or ill feelings towards the company could carry out this attack.

Attacker steals credit card information through payment gateway

- **Damage potential (10)** This would cause a significant financial loss for users.
- **Reproducibility (1)** This threat is very difficult to reproduce as once this threat happens, the company would patch the vulnerability and a new method to break in would have to be found making it very hard.

- **Exploitability (3)** The required knowledge would have to be quite advanced, however on the dark web, malware tools exist to break payment gateway security systems which may work.
- **Affected users (10)** All users who make a payment would be affected.
- **Discoverability (1)** The discoverability of this threat is very low as it is highly privileged information.

The overall risk of this threat is 25 which is high because if an attacker gets access to a user's credit card information, they could steal their money and they could sell this information to other hackers.

Denial of Service attack on the inventory/transactional records

- **Damage potential (4)** The damage potential of this attack is quite average, as it would not necessarily harm anyone, but it would destroy data records which could be bad.
- **Reproducibility (2)** The reproducibility of this threat is very difficult as it would require admin access into the database system.
- **Exploitability (3)** The knowledge required is advanced as attackers would be required to escalate their privilege.
- **Affected users (10)** All users would be affected by this threat as they would not be able to buy products from the vending machine.
- **Discoverability (3)** The discoverability of this threat is low, as they would require admin access to the system.

The overall risk of this threat is 22 which is a moderate risk. The database is quite secure as it requires admin accounts but could be deadly if an attacker got into the database with admin privileges.

MITIGATIONS – PREVENTATIVE, DETECTIVE AND RESPONSIVE CONTROLS

THREAT	PREVENTATIVE	DETECTIVE	RESPONSIVE
Employee physically tampers with dispensing mechanism (Persona / misuse case 2)	The focus is on ensuring employees are being treated fairly and do not have malicious intent towards the company. They need to be paid fairly for their job. This is a good preventative measure as with a good payment, an employee would be satisfied with their job and reduce the chances of rebelling.	The company should monitor employee satisfaction monthly to receive regular feedback on how they are feeling. This method will be able to detect if employees are dissatisfied before it escalates and they have malicious intent.	If an employee has carried out an attack, they have broken a trust boundary. The response to this attack would be to fire them immediately from their job.

COST OF PREVENTIVE MITIGATION

e. Reflection

The processes I used for threat modelling the vending machine were Persona Non Grata/misuse cases, security cards and STRIDE. These three process helped me understand various different threats that were applicable to a vending machine system.

The Persona exercise was effective in identifying potential threats. This process allowed for a high level of creativity to think outside the box for threats by putting myself in the perspective of an attacker. Furthermore, it allowed me to think of various methods that they would use to try exploit the system. This also made it a lot more realistic cause it made me imagine the level of thinking attackers may have that could influence their choices on which parts in particular they would target and why. My answers from this process provided a diversity of threats ranging from a remote cyber-attack by a professional cybercriminal on the payment processing systems of the vending machine to a less complex physical tampering threat. Each of the misuse cases are explained in steps, which helps understand the processes clearly. It was an easy process to apply as it was all about thinking from the attackers perspective. The process can be easily repeated by someone else. It can certainly be applied to other systems as the principles are the same no matter the context, thinking about the type of person who would attack the system, why and how they would do it.

The security card process was also an effective method of identifying threats in the system. It helped me think from different perspectives, especially the motivation cards. They helped me in particular to think about an attackers motives, why they would do it. The stories I created from these cards were detailed and practical. This process also required a lot of creativity. It gave me various options for the different types of security cards and think about how each of those security cards would affect my system if they were applicable. My answers from this process provided a lot of realistic stories with each of the attackers having a different motivation/focus for their attack. The first story involved the attacker being motivated by a financial gain, the second story had the attacker motivated by their belief of physical wellbeing of other users and the third story had no motivation at all where the attacker was simply curious. This covers a range of different motivations that attackers may have for a vending machine attack. The process itself is easy to apply as it gave me ideas whilst I read the different security cards. Furthermore, it is repeatable as the security cards provide very broad ideas and so they can be applied to almost any system.

The STRIDE process was the best method in my opinion for threat modelling. The data-flow diagram (DFD) helped me visualise in detail how the system works and the flows of data between the different components. Performing the STRIDE analysis on this DFD was very comprehensive and it got me thinking about all the flows of data within the system and where there could be potential vulnerabilities. It amazed me how complex a simple vending machine system can get when shown as a DFD. This process didn't require the same level of creativity as the other two processes. It didn't require coming up with stories, instead it was more focused on types of attacks that could occur in different components of the DFD. My STRIDE analysis covered all of the threat categories effectively capturing a range of vulnerabilities in the various components. The methodologies were straight forward to apply, each letter in STRIDE referred to a type of attack and I had to identify the components that were vulnerable to the attack. The repeatability of this process in my opinion is good. It shows how any kind of system can be shown visually using a DFD which allows people to visualise components in any kind of system, no matter how complex. Using STRIDE early in the development of a system allows developers to design systems with security in mind right from the

beginning. Considering threats and mitigations before the system is built would significantly reduce the likelihood of vulnerabilities. Using STRIDE in the vending machine context allowed me to identify at least one type of all the STRIDE attacks, which shows how diverse the attacks can be.

Overall, from these three processes, I learnt a lot about threat modelling and how the different ways to look at systems helps me to identify vulnerabilities in the vending machine system. The overall findings showed that almost all components of the vending machine are prone to attacks, whether they are physical or cyber. This shows the severity of the need for threat modelling for all kinds of systems as they would all have vulnerabilities that need to be identified and to find ways to mitigate and respond to them.