ANALYSIS OF DRONE DELIVERY SYSTEM

COM6017 Security of Embedded and Control Systems

MAY 17, 2019

MANUEL WORLALI ZIWU, ALFRED KUDILIL, SOHAIL AHMED KHAN, RAMEEZ HUSSAIN

Table of Contents

Declaration

The team agree that all members of the team have made reasonable contributions to the work recorded in the report.

Introduction

Throughout the course of the report, we will be identifying different types of threat modelling methodologies and analysing them to find the threats associated with the system. Also, we will be developing a set of security requirements for the system and identifying the major challenges to privacy and safety.

A threat model is a representation of all the issues that affect the security of an application. Threat modelling helps to capture, organise and analyse all the possible threats associated with the system. In addition, the threat model generates a list of prioritised security improvements for the implementation. It is crucial to conduct a threat model on an application as it improves security by identifying vulnerabilities and providing countermeasures to prevent or mitigate the threats to the system.

Security requirements are targets set out for an application at its initiation. Applications are designed differently for different requirements. When these requirements are presented as goals for the final product, the security requirements should also be considered. When building a security requirement, it is crucial to be specific about the types of vulnerabilities to prevent. To produce good security requirements, it shouldn't be imprecise or unattainable. The security requirement should be crafted much like a functionality requirement.

Identification of Threat Models

For threat modelling, we considered different threat modelling methodologies, such as P.A.S.T.A, STRIDE and VAST. After studying the advantages and disadvantages, and comparing these against the requirements of our assignment, we came to a conclusive decision that STRIDE suits more to the task and requirements we have.

Threat Models

P.A.S.T.A

P.A.S.T.A stands for, Process for Attack Simulation and Threat Analysis. It requires seven-step, risk-centric methodology. It stipulates a seven-step process for bringing into line business goals and technical requirements, considering compliance issues and business analysis. The purpose of the threat model is to deliver vigorous threat documentation, list, and scoring procedure. When the threat model is finalised security subject matter specialists develop a comprehensive analysis of the identified threats. Suitable security controls can be scored. It provides an attack-centric view of the application and infrastructure from which defenders can develop an asset-centric mitigation strategy.

VAST

VAST is an acronym for Visual, Agile, and Simple Threat modelling. The main principle of this methodology is the need for scaling the threat modelling process across the infrastructure and entire SDLC and integrating it seamlessly into an Agile software development methodology. The methodology provides options for the exclusive needs of many stakeholders, which can be - application architects and developers, cybersecurity personnel, and senior executives. The methodology provides a unique application and infrastructure visualization scheme, such that the creation and use of threat models do not require specific security subject matter proficiency.

STRIDE

STRIDE is a threat model which was developed by Praerit Garg and Loren Kohnfelder for the purpose of classifying computer security threats. It specifies a mnemonic for security threats which has six categories which are as follows:

- **Spoofing - act of posing as someone else or claiming a false identity**
- **Tampering - malicious modification of data or processes**
- **Repudiation - ability of denying that an action or an event has occurred**
- **Information disclosure - data leaks or data breaches**
- **Denial of Service - causing service to be unavailable to its intended users**
- **Elevation of privilege - gaining access that one should not have.**

Introduction of SHORC System

The objective for Sheffield Amazing On-line Retail company (SHORC) is to deliver items purchased by customers using drones. The company's items are stored in a warehouse in the city.

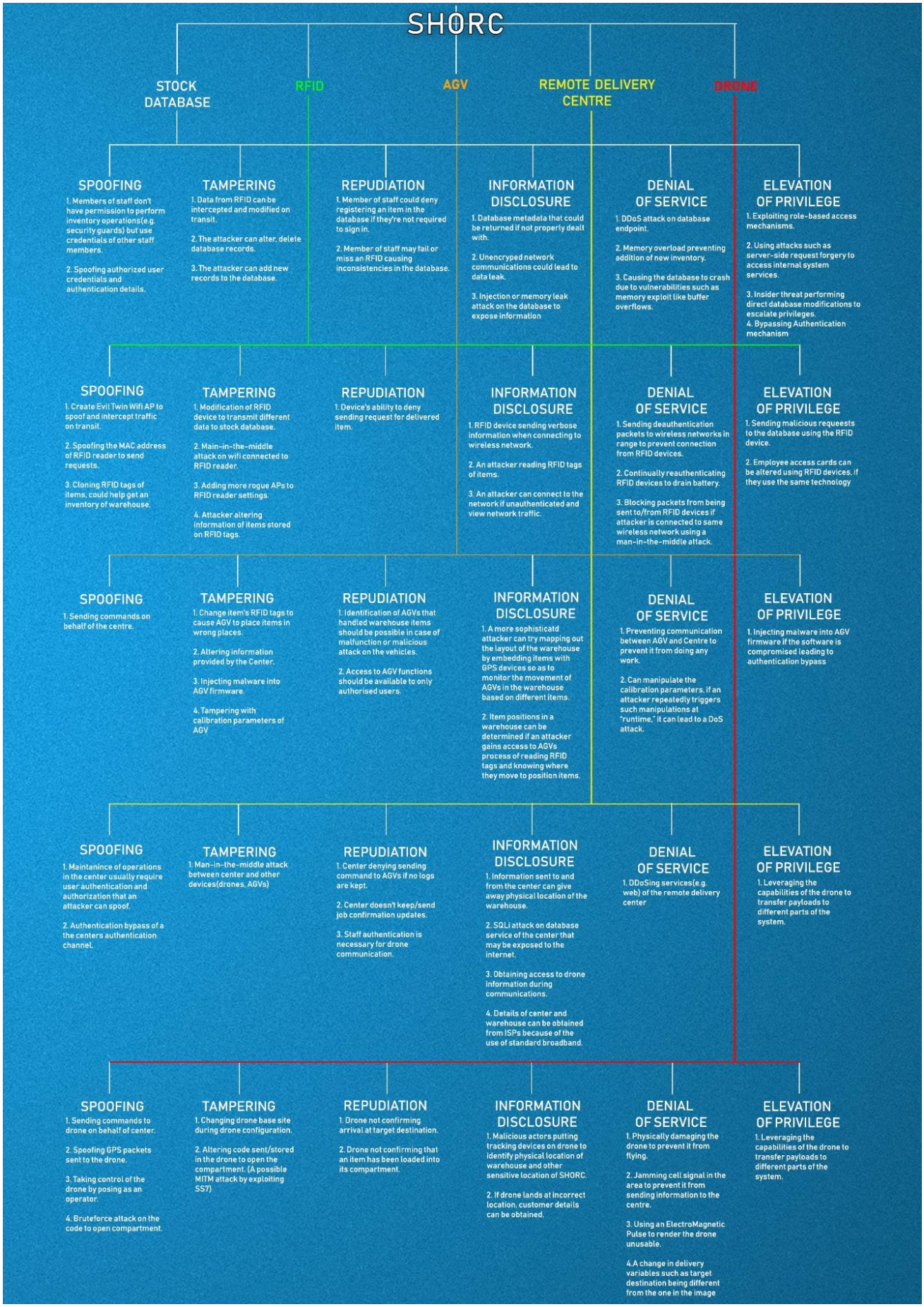
- The warehouse is secured by a fence and staff access the warehouse via a gate.
- Lorries deliver items to the warehouse's reception bay.
- Each item has an RFID tag on it.
- The delivered items are registered into a stock database using a Wi-Fi-ed hand-held RFID reader by a member of staff.
- Automated Guided Vehicles (AGV) are used to take the delivered items and store them in their appropriate storage location within the facility. Also, it retrieves them from the item's storage location to the drone loading bay when it is time for delivery.
- The AGV's inform the Remote Delivery Centre (RDC) about its completion of the job and its availability for further jobs.
- When an item is ready for delivery, the member of staff scans the RFID making sure it is removed from the stock database.
- The item is loaded into the drone's compartment and the GPS and location images are sent to the drone by the centre. The drone then informs with the centre that the item is loaded, and the GPS information has been received.
- The take-off and delivery are issued to the drone.
- The drone had 360-degree cameras for safe landing and take-off. Also, a camera for navigation and location identification.
- The communication between the drones and the centre is via mobile internet. The communication between the centre and warehouse are via high-speed broadband.
- The drone delivery scheme consists of two modes: automated operator and operator assisted. Automated operator mode consists of the drone landing and taking off itself. Operator assisted mode consists of an operator using the camera on the drone to see the live video to operate the drone.
- The customer can open the compartment of the drone by entering the code on the keypad of the drone. The code is sent to their mobiles just before landing.
- The drone informs the centre when the compartment has been opened by the customer.

Identification of Different Features in the System

The first phase in structuring a secure system is to understand and analyse the threats. Threats are possible events that can occur and cause a system to malfunction or respond in an unexpected way. It is vital to classify threats to regulate countermeasures for reducing them. To ease identification of threats, we firstly looked at the different part of the system and the communication between them. Below is a visual representation of the SHORC's threat model.

Finding and Analysing Threats with STRIDE

In this section, threats to the stock database, Wi-Fi RFID reader, AGV's, RDC and drones are classified using the STRIDE model. Below is a flow chart diagram of the threats found using the STRIDE method.



STRIDE Threat Model Applied to Stock Database

SPOOFING

- Identity Spoofing - Identity spoofing is whereby an entity taking the identity of another entity to achieve a goal. Within the company, some employees are not authorised to perform inventory operations. For example, security guards and other non-office employees. However, they can obtain credentials of authorised employees and use them to gain privileges to perform such operations.

- Action Spoofing - Action spoofing is whereby one action is being disguised for another; tricking users into initiate an action they didn't intend to. An attacker can obtain credentials and redesign the stock database for malicious purposes. For example, a user can be tricked into believing that clicking a specific button will update the stock database, but in fact, it deletes the database or downloads malicious content.

TAMPERING

- Man-in-the-middle attack - Man-in-the-middle attack is whereby an attacker can get in between communication and possible spy or alter the data. For example, data sent from the RFID reader to the stock database can be intercepted and altered during transit.

- SQL injection - SQL injection attacks can allow attackers to spoof identity and tamper with the database, which compromises the disclosure of data in the system. For example, the attacker can modify, delete database records and add new records.

REPUDIATION

- A member of staff could deny the fact of registering an item in the database if they're not required to sign in. They could possibly get away with it as there is no solid evidence.

- A member of staff could possibly fail or miss an RFID which can lead to inconsistencies in the database.

INFORMATION DISCLOSURE

- The metadata from a database could be returned if it's not properly dealt with.
- Network communications that are not encrypted could lead to a data leak
- SQL injection or a memory leak attack on the database can lead to exposure of information.

DENIAL OF SERVICE

- Resource exhaustion attack - Resource exhaustion attack is whereby security vulnerabilities cause a computer to crash, hang or interfere with a specific system or program. For example, an attack like this could lead to a system that runs the database to crash and corrupt the database.

- XML denial-of-service attack - An XML DoS attack is whereby the purpose of it is to shut down a web service or a system that runs it. For example, the database service or the system or running it could be shut down and possibly corrupted if not done properly.

- Buffer Overflow – Buffer overflow is whereby an attempt is done to put more data in a buffer more than its capacity, which can lead to corruption of data or even execution of malicious code. For example, this can be executed to change the execution path of the SHORC application by overwriting some parts of its memory. This will cause the application to crash.

- Network flooding - Network flooding is whereby every incoming packet is forwarded from one node to every other node linked to the router. For example, an attacker can bring down the network and service by flooding it with large traffic. This could be done via the Wi-Fi handheld reader or through the communication via mobile internet, which could cause to flood large amounts of traffic through the network channels.

ELEVATION OF PRIVILEGE

- Exploitation of role-based access mechanisms.
- A server-side request forgery attack can be used to access internal system services.
- Insider threat could perform direct database modifications to escalate privileges.
- Authentication Bypass – Authentication bypass is whereby an attacker obtains access to a service, application or device with privileges of an authorised user by avoiding an authentication mechanism. For example, an attacker or employee can bypass the authentication mechanism in the computer.

STRIDE Threat Model Applied to Wi-Fi RFID Reader

SPOOFING

- An attacker or employee can create an Evil Twin Wi-Fi AP to spoof and intercept traffic on transit.
- The MAC address of RFID reader can be spoofed to send requests.
- The RFID tags of items can be cloned to obtain the warehouse in inventory.

TAMPERING

- The RFID device can be modified to transmit different types of data to the stock database.
- The Wi-Fi connected to the RFID reader can be prone to a man-in-the-middle attack.
- More rogue Aps can be added to the RFID's reader settings.
- An attacker or employee can alter the information of the items stored on RFID tags.
- A fake cloned RFID tag can be used on store items instead of legitimate ones.

REPUDIATION

- The device's ability to deny sending requests for delivered items.

INFORMATION DISCLOSURE

- The RFID device can send verbose information when connecting to a wireless network.
- An attacker or an unauthorised employee can read the RFID tags of item.
- An attacker or an unauthorised employee can connect to an unauthenticated network and view the network traffic.

DENIAL OF SERVICE

- De-authenticated packets can be sent to wireless networks in range to prevent the connection from RFID devices.
- The RFID device can be continually reauthenticated to drain the battery.
- Through a man-in-the-middle attack, an attacker could connect to the same network as the RFID device to block packets from being sent to and from the RFID device.

ELEVATION OF PRIVILEGE

- The RFID device can be prone to sending malicious files to the database.
- RFID devices can be used to alter employee access cards if they use the same technology.

STRIDE Threat Model Applied to Automated Guided Vehicles

SPOOFING

- Sending commands on behalf of the centre

TAMPERING

- Change the item's RFID tags to cause the AGV to place the items in the wrong places.
- Altering information provided by the RDC
- An attacker or unauthorised employee can inject malware into the AGV firmware
- Tampering with calibration parameters of the AGV

REPUDIATION

- AGV's not confirming job confirmation updates with the RDC.
- AGV'S not showing what items are currently in transit to the RDC.

INFORMATION DISCLOSURE

- An advanced attacker can possibly try mapping out the layout of the warehouse by embedding items with GPS devices so it will monitor the movement of AGV'S in the warehouse based on different items.

- The storage location of the items in a warehouse can be determined if an attacker gains access to the AGV's process of reading RFID tags and knowing where they move the items to.

DENIAL OF SERVICE

- Preventing communication between AGV and the RDC to prevent it from doing any work.
- The calibration parameters can be manipulated if an attacker repeatedly triggers such manipulations at "runtime". This can then lead to a denial of service attack.

ELEVATION OF PRIVILAGES

- Malware can be injected into the AGV firmware if the software is compromised leading to authentication bypass.

STRIDE Threat Model Applied to Remote Delivery Centre

SPOOFING

- An Identity spoof whereby the attacker can spoof the user authentication and authorisation at the centre's maintenance of operations.
- Authentication bypass of the centre's authentication channel.

TAMPERING

- Through a man-in-the-middle attack, an attacker can spy or alter data of the communication. between the centre and other devices, e.g. drones, AGVs.

REPUDIATION

- The RDC denying sending job commands to AGVs if no logs are kept.
- The RDC fails to keep/send job confirmation updates.

INFORMATION DISCLOSURE

- The information being sent to and from the centre can reveal the physical location of the warehouse.
- SQLi attack on database service of the RDC may be exposed to the internet
- Gaining access to the drone information during the communication between the RDC and drone.
- Details of the RDC and warehouse can be obtained from ISPs because of the use of standard broadband used for communicating.
- Communication with the mobile device can be intercepted by exploiting an SS7 vulnerability.

DENIAL OF SERVICE

- Through the use of resource exhaustion attack, the RDC servers can be shut down.
- An XML denial of service can be used to shut down or corrupt the RDC web service or the system that runs the service.

ELEVATION OF PRIVILEGE

- By bypassing the authentication, the attacker can gain unauthorised remote access to the centre by exploiting a vulnerability in any service that are not protected.

STRIDE Threat Model Applied to Drones

SPOOFING

- Resource Location Spoofing – Resource location spoofing is whereby an attacker deceives
- Counterfeit GPS Signals – An attacker can deceive a GPS receiver by spreading counterfeit GPS signals to resemble a normal GPS signal. For example, the drones GPS location can be spoofed to show the drone in another place, rather than the place it actually is.
- Carry-Off GPS Attack – A carry-off GPS attack begins with an attacker sending signals combined with genuine signals observed by receiver. The attacker can carry the target away from its intended location to a location chosen by the attacker. For example, the drones GPS signals can be synchronised with the attacker's signals for the drone to land somewhere else rather than the place it is intended to.
- Through identity spoofing, the attacker can act as the drone controlling operator.
- Brute force attack can be used to crack to the code and open the compartment.

TAMPERING

- Changing the base site of the drone during the configuration stages of the drone.
- Alteration of the code sent/stored in the drone to open the compartment to acquire the item. This can be known as a man-in-the-middle attack by the exploitation of SS7.
- Changing the target delivery information from the RDC

REPUDIATION

- Drone not confirming arrival status at target location with the RDC.
- Drone not confirming that an item has been loaded into its compartment with the RDC.

INFORMATION DISCLOSURE

- The physical location of the warehouse and other sensitive locations can be revealed to the attackers if they placed a tracking device on the drone.
- In unfortunate cases, if the drone lands at an incorrect location the customer details will be revealed.

DENIAL OF SERVICE

- Damaging the drone physically, e.g. throwing a rock at it, can prevent it from flying.
- Jamming the cell signal in the area to prevent the drone's communication the RDC.
- An Electromagnetic Pulse can be used to make the drone unusable.
- A change in delivery variables, such as the target destination being different from the one in the image can be prevent the drone from delivering the package.

ELEVATION OF PRIVILAGES

- Leveraging the capabilities of the drone to transfer payloads to different parts of the system.

Development of Security Requirements

Security requirements are security features that are a requirement by users of the system or the quality the system must have to increase the trust of the user in the system they use. The physical, logical and procedural aspects of the system were used to develop the set of security requirements.

Physical Security

Physical security is usually a vital concern in facilities that has a lot of assets. Physical security provides countermeasures to ensure the protection of resources, such resources include computer equipment, personnel and other properties from unauthorised physical access and damage. In addition to that, it provides countermeasures against physical threats such as vandalism, fire, natural disasters and theft. Physical security consists of two phases, deterrence and detection. Deterrence phase consists of the different types of methods and measures that are meant to protect assets from attackers, intruders or natural disasters. Detection phase consists of allowing security employees to detect and locate intruders using cameras, security lights, motion sensors and watch dogs.

Requirements

- Security gates must be well-protected and equipped with alarm systems to prevent thieves or unauthorized access into SHORC facilities such as the warehouse or Remote Delivery Centre.

- All drone compartments and other important parts such as keypads and sensors must be enclosed in a case and protected in case the drone lands forcibly or at an unintended location.

- Automated Guided Vehicles must have physical constraints such as locked cases to protect any interfaces such as serial or JTAG that may allow installation of malicious firmware.

- Protection of physical equipment from theft and compromise of IT facilities by physical means must be protected by locking up equipment after the end of a word day and constantly monitoring facilities with CCTV Cameras.

Logical Security

Alongside physical security standards in place, logical security should also be considered to make it more effective. Logical security consists of the specific controls that are put into place to manage access to computer systems within the data centre, e.g. having a locked door to protect the server room is physical security but having a two-factor authentication alongside will make it a form of logical security. This method can be used within computer systems in the data centre. Passwords do provide restricted access to authorised employees, but to make it more effective, restriction on who can access what content is essential. These requirements are to prevent unauthorised access to the assets and data from former employees or employees that are not authorised.

Requirements

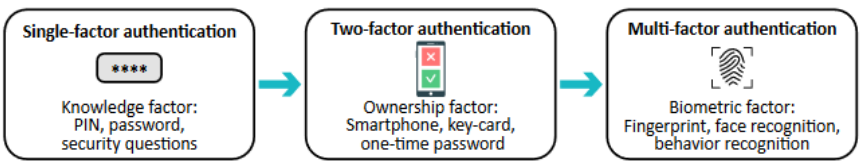
- Various staff's access rights must be put in place such as different access rights for receiving an item and registering the item in the database. A user-based role model [1] will be the best way to provide different access rights to various members of staff in the warehouse and Remote Delivery Centre.

- Staff must be able to identify themselves using means such as biometric data or electronic means like RFID cards before being allowed to different parts of the facilities and use of various equipment. It is also important that these include different access rights for the members of staff. Additionally, this can be extended to lock employee workstations when they are aware of them [2].

- Drones must be provided with a method of authenticating themselves when they arrive at their base site before connecting to any devices on the network to prevent intrusion by rogue or compromised drones. Additionally, any wireless adapters that aren't required for communication such as Bluetooth adapters and Wi-Fi adapters should be removed from the drones.

- Any firmware updates to the AGV must be from an authorized source. This can be enforced by only installing firmware that is signed form a trusted authority. Furthermore, it must be ensured that any firmware updates come from a trusted source and the AGV should be able to self-authenticate any firmware before installation [3].

- Strong password policies must be implemented in every part of the system that requires authentication. Furthermore, members of staff that have physical access to network devices and require authentication to use them, must employ multi-factor authentication [4].



Procedural Security

Procedural security consists of guidelines and agreements that advise people to act in specific ways with the intention or goal of proof protecting assets. Moreover, procedural security entails procedures such as regulations, organisation policies, guidelines, copyrights, patents and trade secrets. It relies on users to follow specific rules or perform certain procedures that are not required by physical and logical means.

Requirements

- Security guards must that all personnel entering the warehouses must be authorized and should have permission to get into the facility. This must include any unexpected guests that may claim to come from "management".

- Member of staff must also be trained to know not to help individuals get into places by tailgating them. Tailgating is an act where a person without access follows closely behind someone with access to get into restricted places. In addition to this, regular training exercises should be done to raise awareness and protect members of staff from social engineering attacks such as phishing [5].

- Items that have not been stored in the database (i.e. items that haven't been scanned by the RFID reader) should not be placed in storage locations by Automated Guided Vehicles. This can be done by ensuring that upon delivery by the lorries, the manifest of delivered items must tally with any updates or new items in the stock database.

- Any software or firmware updates must go through a rigorous process of tests by security experts. Only a set number of people should be allowed access to code repositories and making updates to any equipment.

- Data stored on drones must be wiped after every complete delivery and drone configuration must be checked for any alterations. Likewise, the drone must be thoroughly checked for any foreign object by members of staff before being used again.

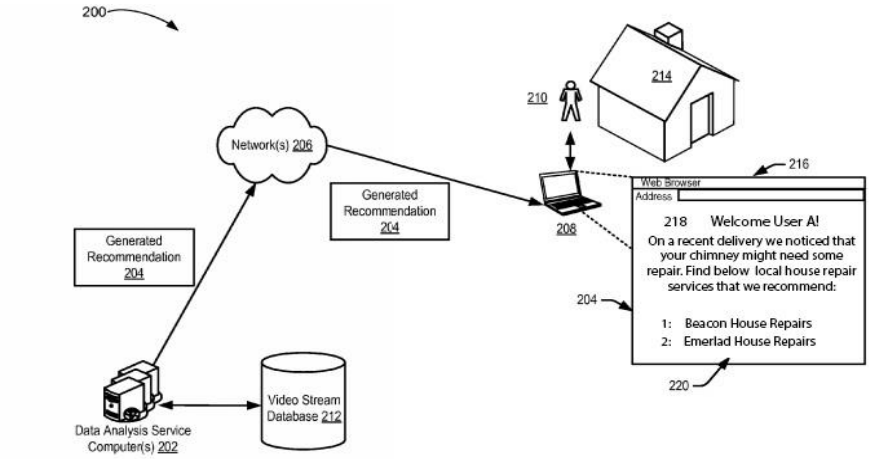
- Foreign devices such as RFID readers, drones and computers should not be allowed to connection to the network of the system. It must be ensured that any exceptions to this does not include malicious programs or devices that could compromise the network.

Major Challenges to Privacy

In most areas of data collection, more often than not there is the issue of privacy as to what data is allowed to be collected and what it is being used for. Drones are a major component o the system which can uncontroversially cause privacy concerns. It is now very common to hear a lot about companies invading the privacy of customers especially online for financial gain. More recently, stricter privacy laws have been created to protect individuals from mass data collection by large organizations. The use of drones is no exception to hit, as drones are usually equipped with cameras that capture images for better navigation. However, these cameras can be used to gather more information than is necessary about the current and potential customers. Another aspect of the system that could be an invasion of privacy to customers is the data stored on them in relation to their purchase history. This gathered information can later be used to serve them with specifically crafted ads and suggestions.

Drone Privacy Concerns

A major privacy concern of the system could be that people mistaking the drone as one used for information gathering or surveillance purposes. This is unfortunately not far-fetched as it is common for government organizations and large corporations to use such equipment for surveillance and information gathering to gain a financial advantage over their competitors [6]. Information gathering with drones can be done by video recording or by capturing images which can be analysed to serve customers with targeted advertisements. An example is notifying a customer about a damaged chimney on their roof or recommending a service to attend to a cracked driveway [7].



Drone Privacy Recommendations

The company must implement public privacy legislation that requires transparency to protect citizens' privacy and neutralize public perception towards drones and specifically delivery drones. Implementation of geo-fencing restrictions to limit data capturing to delivery recipients only and prevent the gathering of large amounts of data by a single entity/drone. In addition to this, any privacy legislation should follow GDPR guidelines accordingly [8]. This must include the ability for customers to delete their personal data and regular deletion of image and video data that can be used to specifically identify private details captured by drones in transit.

Conclusively, the absolute challenge will be to overcome negative public perception privacy towards drones [9]. The reality, however, is we have already overcome psychological barriers similar to this in the past such as with driverless cars and smart homes.

Stored Data Privacy Concerns

In addition to public privacy concerns in relation to drones, data stored on customers and orders may cause an invasion of privacy in case of a database breach or inappropriate access by a member of staff. For example, operators who control drones for delivery or IT team of the company being able to access data of customers' personal details and order details simultaneously.

Stored Data Privacy Recommendations

In a similar fashion as with the drones, the company must also have a Data Protection Legislation which protects the personal data of its customers from privacy infringements. The Data Protection Legislation must keep customers data accurate, safe, secure and lawful [10]. The company should define some authorization privileges for the members of staff. It should be ensured that members of staff that load drones with items for delivery are not given any information that relates the item to the intended customer. This can be done by equipping the drones with devices that imprint customer details on packages upon loading. Moreover, drone operators should not be allowed access to certain drone functionalities such as RFID readers or the database that could allow them to identify items being delivered to the required target.

Major Challenges to Safety

It is imperative that challenges to safety posed by any system should be identified and dealt with accordingly. SHORC is no exception to this, and some major challenges to safety have been identified at certain aspects to the system. These include: the drone, the Automated Guided Vehicle and the safety in the warehouse itself.

Safety challenges in the drone

The drone is a major part of the system where safety is of importance with regards to the public. Drone usage is growing at a rapid rate in the skies and some of the busiest anywhere in the world. A new trend is growing as drones are now being used to deliver items and safety challenges with the public must be dealt with.

Issue: Flight paths taken by the drone must be carefully chosen to prevent drones from colliding with commercial aircrafts which would cause massive loss of lives [11]. This can automatically be addressed if the drone is in autonomous mode but could be a problem if there are no restrictions with the drone being in operator mode. Likewise, operating the drones at low altitudes could pose a safety risk to personal property and individuals, for example, crashing the drone into buildings or individuals [12]. Damage to the drone's camera or it's inability to provide visual feed to the drone operator would make drone control difficult; this can also be difficult if the drone is in autonomous mode preventing it from identifying and bypassing any obstacles in its path. Similar concerns are met when the drone is exposed to poor weather conditions and perhaps even worse if the drone is not water-resistant and could be an electric and fire hazard [13].

Solution: It is vital that the drone operator keeps clear and does not interfere with any aircraft operations. The drone should not be flow over or near sensitive infrastructure such as power stations. The Drones Laws UK 2018 contains guidelines on how drones can be used and has been implemented for safety regulation purposes regulated by the Civil Aviation Authority (CAA). In addition to this, a failsafe can be implemented that overrides and limits the height a drone can get to even when in operator mode. This can be implemented in the Altitude Hold mode that is common with most drones [12]. A safety documentation should be provided for drone operators and other members of staff. Proper safety and regular maintenance of the drone must be done regularly to avoid any potential accidents that might occur from malfunctioned equipment.

Issue: In a situation where drones are not well-maintained, there is a risk of drone components that could be easily detached as well as items deployed for delivery. This is a major safety concern as these drones as likely to operate in residential areas where the risk of objects falling on civilians under these circumstances are high [11].Furthermore, the drones have blades that are required for flight; but could be harmful or could break off if they strike a hard surface.

Solution: The camera is one of the major ways of letting an operator know of any obstacles that could be in the path of the drone. This would not be much of an issue if the drone is in operator mode but could pose a safety challenge to people around and the drone as a whole. The use of computer vision techniques such as image recognition could help prevent any accidents that could occur in that regard. Without the ability to detect and avoid obstacles, the drone is more likely to crash into buildings and people [14]. The drone should be equipped with emergency parachutes that are automatically deployed during unforeseen circumstances such as when the drone is moving haphazardly as detected by the internal gyroscope, to reduce crash damage and any potential injuries [14].

Safety challenges in the Automated Guided Vehicle

Unlike safety concerns with the drones, that is largely focused on the public, challenges to safety with the AGV is more of an issue with members of staff that work in the warehouses of SHORC.

Issue: One of the obvious major safety concerns with regards to the AGV is physical injury that it can cause members of staff in the ware house. It is vital for any control system to know its current position and make decisions accordingly. In this regard, the AGV must also be able to detect the presence of arbitrary objects in its path and stop from colliding into them.

Solution: The AGV should be constantly monitored regarding its speed and position in case of odd behaviour and unexpected movements [15]. This can be done by using cameras that are monitored by the Centre and sending remote commands to stop AGV operations when necessary. The AGV should also send information about its state and operational mode regularly.

Issue: Precision is a must when dealing with industrial control robots or automated systems that have a direct interaction with the physical world. Any misconfiguration or faults in the AGV could result in a potential life-threatening situation. An example of this can be when the AGV has to interrogate an item using its RFID; and the AGV misreads the data and misplaces the item in the warehouse. Besides the obvious case of its difficulty to locate, there is also a safety concern where items could be unbalanced and topple over shelves or cause entire rows of items to fall in the warehouse.

Solution: Maintenance of the AGV must be done regularly to prevent any unexpected behaviour that may arise from old and/or faulty equipment. Regular tests should also be done to ensure optimal operation of the AGV before it is used. Finally, the warehouse as a unit may contain materials that could be a safety hazard to members of staff. Fire outbreaks could harm members of staff and the risk of falling objects is still an issue. Correct building permits and proper fire safety measures such as staff training and installation of automatic sprinkler systems should be put in place to help prevent and reduce any possible harm that can be caused.

Conclusion

This paper proposes a threat model for an online retail company. Several threat model architectures are considered in finding threats for the system but the more popular STRIDE threat model is used to identify potential threats that the system may have. Moreover, privacy and safety concerns that may pose challenges to the company are identified and analysed with the proposed countermeasures of dealing with them. In addition to this, security requirements are proposed to reduce the possibility of a successful cyber attack on the company. Various aspects of the system are provided with physical, logical and procedural security requirements.

References

[1] T. Mudarri, “Security Fundamentals: Access Control Models,” *Internal Jornal of Interdisciplinarity In Theory And Practice,* p. 261, 2015.

[2] I. &. M. A. Alsmade, “Improving Enterprise Access Security Using RFID,” *International Journal of Computer Science and Information Security,* vol. 9, 2011.

[3] L. Shade, “Implementing Secure Remote Firmware Updates,” 2011.

[4] S. B. N. M. S. A. T. M. Y. K. Aleksandr Ometov, “Multi-Factor Authentication: A Survey,” *MDPI,* 2018.

[5] G. S. Hussain Aldawood, “Reviewing Cyber Security Social Engineering Training and Awareness Programs == Pitfalls and Ongoing Issues,” *Future Internet,* 2019.

[6] D. C. C. K. McKelvey N, “Drones and Privacy,” *International Journal of Handhelp Computing Research,* vol. 6, pp. 44-57, 2015.

[7] Greene T, “The Next Web,” The Next Web, 24 August 2017. [Online]. Available: https://thenextweb.com/tech/2017/08/24/amazon-patent-details-the-scary-future-of-drone-delivery/. [Accessed 11 May 2019].

[8] Information Commisioner's Office, [Online]. Available: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. [Accessed 12 May 2019].

[9] “Drone Deliveries are Not Longer Pie In The Sky,” Forbes, 10 April 2018. [Online]. Available: https://www.forbes.com/sites/startupnationcentral/2018/04/10/drone-deliveries-are-no-longer-pie-in-the-sky/#62b28b341880. [Accessed 12 May 2019].

[10] “Why is data protection so important? - Legislation, security, and consequences for businesses,” Fsb, 6 February 2017. [Online]. Available: https://www.fsb.org.uk/resources/why-is-data-protection-so-important. [Accessed 13 May 2019].

[11] M. R., “Are Drones Safe? Here's 5 Things To Think About.,” [Online]. Available: https://diydrones.com/profiles/blogs/are-drones-safe-here-s-5-things-to-think-about . [Accessed 24 April 2019].

[12] “Altitude Hold Mode,” Ardupilot, [Online]. Available: http://ardupilot.org/copter/docs/altholdmode.html. [Accessed 15 May 2019].

[13] L. Mark, “Tips for Flying Your Drone in Sub-Optimal Weather Conditions - dummies,” Dummies, [Online]. Available: https://www.dummies.com/consumer-electronics/drones/tips-for-flying-your-drone-in-sub-optimal-weather-conditions. [Accessed 12 May 2019].

[14] M. Malek, “5 Technologies Improving Drone Safety,” DroneLife, 23 January 2019. [Online]. Available: https://dronelife.com/2019/01/23/5-technologies-improving-drone-safety/. [Accessed 29 April 2019].

[15] H. Steven, “7 Industrial Robotics Hazards and How to Avoid Them,” Bastian Solutions, [Online]. Available: https://www.bastiansolutions.com/7-industrial-robotics-hazards-and-how-to-avoid-them/. [Accessed 26 April 2019].

[16] S. Brancdorn, “When a Drone Crashes into an Airplane, Everyone Has a Bad Time,” Live Science, 15 October 2018. [Online]. Available: https://www.livescience.com/63828-drone-crashes-into-airplane.html?fbclid=IwAR2Tq0ReOZ2ebXyrSI0OQlvZIgRVLd6ooPxB31KGDJU4V7sAdRWy-SonSbk. [Accessed 14 May 2019].