COM6017 Security of Embedded and Control Systems

Analysis of a Drone Delivery System

Kai Zhang

David Kennedy

Min Hu

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

Contents

Introduction

Report Structure

The analysis of this report considers a retail sector drone-based delivery system. Sheffield Amazing On-line Retail Company, (SHORC) which uses aerial drones and automated guided vehicles (AGV's) to deliver parcels bought by customers who are able to provide appropriate drone landing sites.

SHORC's delivery chain contains numerous areas which could contain cyber vulnerabilities. By first detailing the topology of the delivery system, possible vulnerabilities and the method of how they could be exploited will be explored using a STRIDE threat model. A set of security requirements covering physical, logical and procedural requirements will then be produced from the explored vulnerabilities. These produces if implemented by SHORC will aim to mitigate or eradicate the financial, operating and reputational damage should these vulnerabilities be exploited.

An autonomous delivery system provides major challenges to the privacy and safety of not just the recipients of the deliveries but to the general public as a whole. Some of these concerns will be outlined along with possible solutions that seek to reduce the public's concern about drone delivery systems.

Identification of Threats within the System

Topological Overview of SHORC System

This section will introduce an overview of the SHORC delivery system, outlining the key components of the structure and how these components interact with each other this is shown in figure 1.

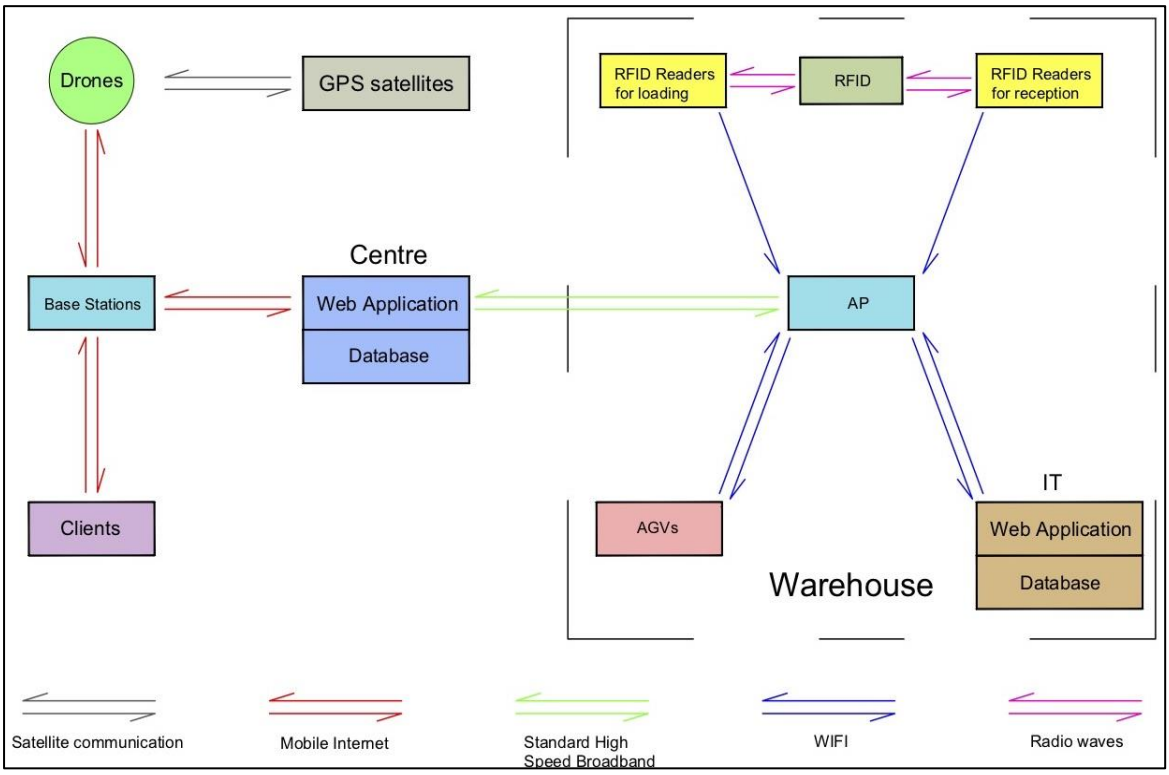


Figure 1: Diagram detailing the key components of the SHORC delivery system and how these components interact with each other. The AP in this diagram are the access point WiFi routers within the warehouse that allow components to communicate with the Stock Database and the Order Database stored at the Centre.

Responsibilities of Components in the SHORC System

Each component within the system has specific responsibilities to ensure the automated deliver process runs smoothly, understanding these responsibilities is key to finding vulnerabilities within the system. The system components and their corresponding vulnerabilities are shown in table 1, with further diagrams of component communication in the following section.

ID	Component		Responsibilities
1	**RFID Readers**		· Read the RFID on the parcels and update the stock count in the database. · Read the RFID on the parcels at the loading bay and remove the stock count from the database.
2	**RFID**		· Store information related to the content of the parcel
3	**IT**	**Web Application**	· Transmit the data regarding the availability of parcels sent by the RFID Readers to the stock database as a PUT request. · Send a response about whether a parcel is in stock after a request from the remote delivery centre. · Send a response containing a parcels storage location to an AGV when a request has been made by the AGV.
		Stock Database	· Stores information relating to the number of parcels in stock.
4	**AGV's**		· Place the parcels delivered at reception to the correct location in the warehouse. · Take the parcels from the storage location to the drone loading bay.
5	**AP**		· An Access Point, networking hardware device that allows other Wi-Fi devices to connect to the network.
6	**Remote Delivery Centre**	**Web Application**	· Determine whether parcels on an order are in stock and whether an order can be fulfilled. · Schedule when the orders should be delivered. · Create tasks for the AGV's. · Supply the drones with delivery information, take-off clearance and delivery authorisation · Manage the status of all drones and AGV's, request on board information.
		Order Database	· Store information about clients, such as address, orders, purchase history, landing site pictures. · Store information about the status of the AGV's and drones. Such as availability, battery state and reported location. · Store weather information.
7	**Base Station**		· Handles the mobile communication between the remote delivery centre, clients and the drones.
8	**Drones**		· Safely take the parcels from loading bay and navigate to the delivery landing site coordinate. · Determine whether it is safe to land and take-off. · Store a copy of the passcode and verify whether the passcode matches the one entered by the client. If so open the parcel compartment. · Return to the warehouse loading bay after delivery.
9	**Clients**		· Place the order. · Remove parcels from the storage compartment according to the code sent by the centre.
10	**GPS satellites**		· Provide the drones with reliable information regarding their position.

Table 1: Table displaying a breakdown of the components shown within the system diagram of figure 1 and their corresponding responsibilities.

Detailed Explanation of Communication between Components

The basic process of how parcels are processed through the warehouse is that parcels are transported from the manufacturer and delivered to the reception. These parcels are then stored within the warehouse shown in figure 2. The orders are collated, shown in figure 3, with the parcels removed from storage and delivered to the recipient, shown in figure 4.

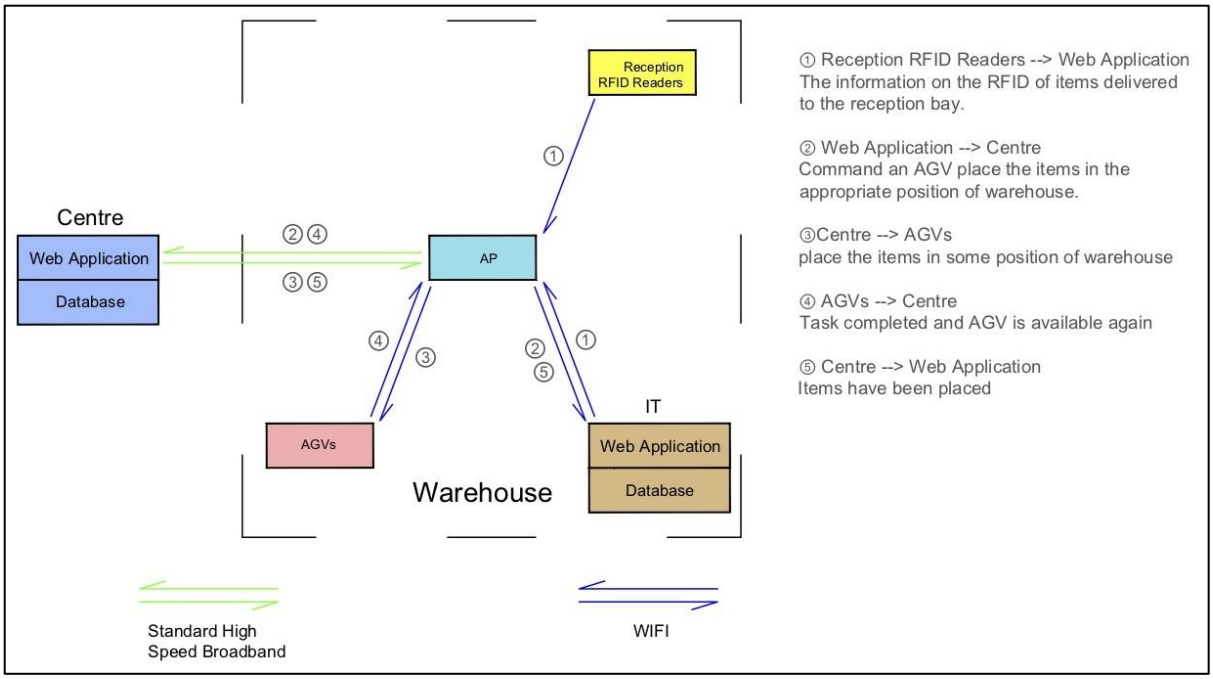


Figure 2: Diagram explaining the process of how parcels are moved from the reception to their storage locations in the warehouse.

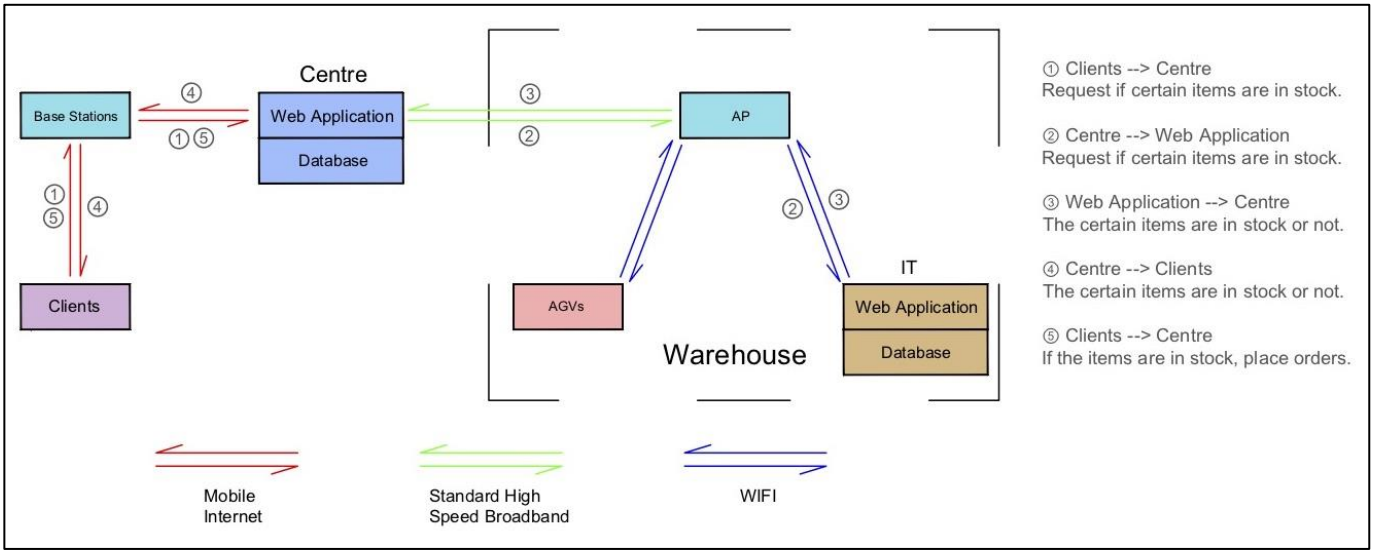


Figure 3: Diagram explaining the process of how the remote delivery centre processes pending orders.

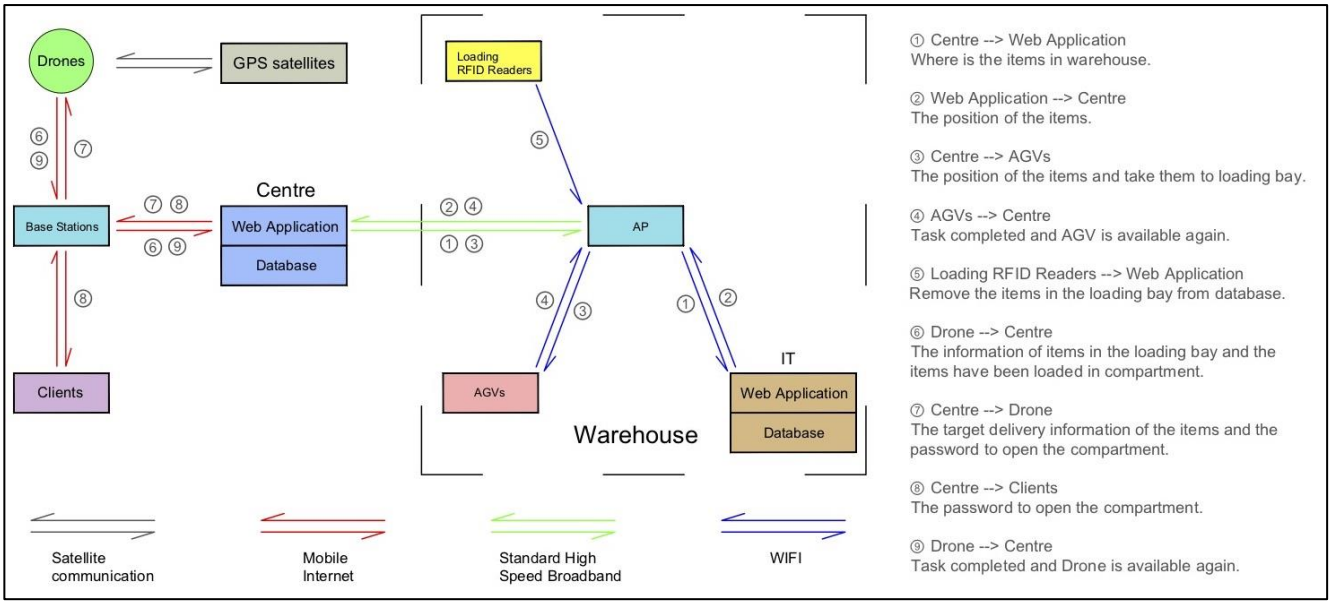


Figure 4: Diagram explaining the process of how the delivery of parcels to the client is fulfilled.

In most cases the parcels are to be delivered to the clients via the drone operating in automated mode. In abnormal situations such as bad weather or unclear landing sites the drone can be manually controlled by an operator. The operator uses the remote delivery centre to control the drone, the remote delivery centre is also responsible for any software upgrades the drone may require. The communication between the drone and the remote delivery centre us shown in figure 5.

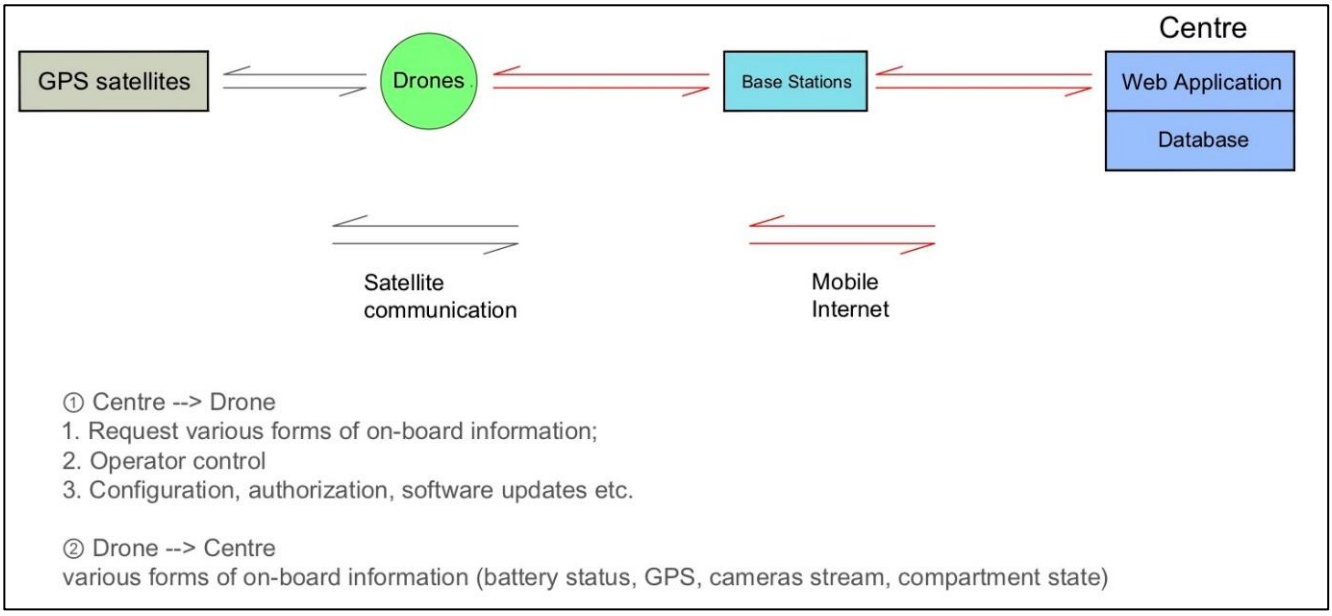


Figure 5: Diagram explaining the process of how the remote delivery centre and drone communicate.

Threat Model

STRIDE has been used as the threat model for this system analysis. STRIDE strands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**valuation of privileges. System components such as the drones have many possible attack vectors, in this model vulnerabilities have been found that are specific to the SHARC system. It is also the responsibility of the manufacturers of the selected drone model for example to account for possible attack vectors present in drones.

Threats to RFID Tags

RFID tags are present on all parcels within the warehouse, they are interrogated by the RFID readers at reception and the landing bay, the AGV's and the drones. The RFID's store information about the parcels contents, attacking this information could lead to major problems within the delivery processes. For example a malicious users could purchase their own or use a staff RFID readers to read, modify or erase the information in the RFID.

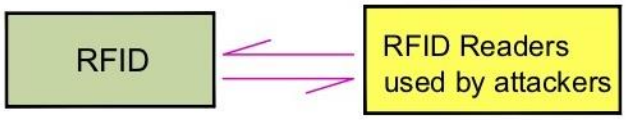


Figure 6: Diagram explaining the process of how RFID readers could exploit RFID tags

Vulnerability	Category	Method	Impact
Data can be sniffed from the RFID tags and used in further vulnerabilities.	**Information Disclosure**	RFID readers can be bought cheaply and used to scan many types of RFID. The parcels are delivered to the reception, if a regular person enters the reception to ask a seemingly harmless question they might have an RFID readers in their bag. They would then be able to gather information from any RFID tags that are attached to the parcels present in the reception.	The metadata such as the storage location of parcels can be exposed and used in further vulnerabilities. Furthermore, the RFID signal can be collected and used in replay attacks or reverse engineered.
Malicious data can be written onto RFID tags.	**Tampering**	The RFID's installed onto delivered parcels are installed offsite. These RFID's could contain malicious data such as SQL Payloads. Many RFID readers are also capable of writing to RFID's, if an RFID reader is exploited then data on the RFID could be re-written.	· New storage locations could be written onto the tags. Parcels that are of a high value could be stored in the location of a low value parcel. When the low value parcel is purchased the buyer receives the high value parcel instead. · Malicious payloads or code could be written onto the tags. When the RFID is read by a reader the payload could be used for injection attacks on the database. · The RFID could simply be destroyed, meaning the parcel cannot be registered or traced in the system and must be sent back to the supplier.

Vulnerability	Category	Method	Impact
RFID tags can be Jammed	**Denial of Service**	Frequency Jammers can be purchased on the internet. To determine the frequency used by the RFID tags, one would have to purchase a parcel and then interrogate the RFID attached with an RFID reader such as a mobile phone. Any jammers placed in parcels delivered to the reception or placed in the vicinity of the reception, would stop all communication between the RFID tags and the readers.	Jammers would effectively stop all processes in the Warehouse and Drone Bay. Parcels could not be interrogated so the storage locations would not be known and so parcels would backlog in the reception area. Workers at the drone bay would not know whether the parcel being loaded onto the drone are the correct ones for the order.
Altering the information could lead to the Warehouse claiming they never received a delivery	**Repudiation**	Exploited RFID readers or fake RFID tags could write or contain data related to other parcels. Therefore, the warehouse may believe that they did not receive the correct parcels from the manufacturers.	This would mix up what parcels are stored in which locations, effectively denying access to some products which would be marked as out of stock. Recipients could receive the wrong parcels and the supplier would have to send more stock to the warehouse.

Threats to AGV's

AGV's are used to transport all parcels around the warehouse, they clearly pose a safety threat to any workers within the warehouse if vulnerabilities are exploited. Vulnerabilities could also cause damage to the AGV's themselves, the parcels they are carrying or the warehouse contents. Most of the vulnerabilities surrounding the AGV's stem from the way the AGV communicates with the remote delivery centre, an example of some of these attack vectors are shown in figure 7.

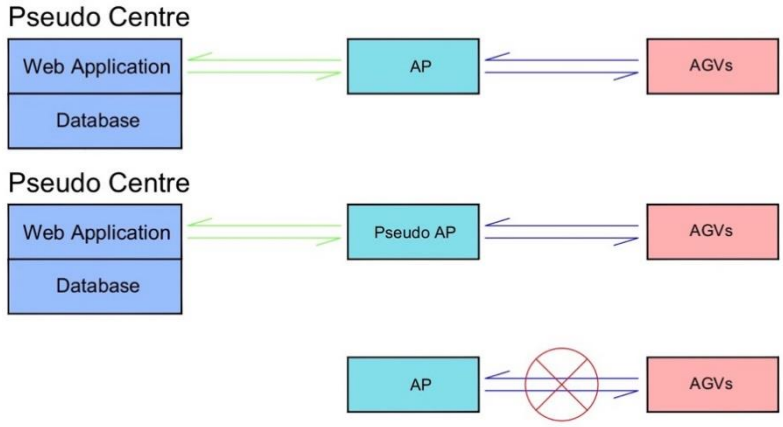


Figure 7: Diagram explaining the process of how the AGV's could be exploited. The top most diagram represents how a fake remote delivery centre could provide incorrect information to the target AGV. The second shows how a fake access point could provide malicious information to the AGV. The bottom diagram shows how the AGV could be denied any information at all.

Vulnerability	Category	Method	Impact
Loosen the brakes on the AGV	**Tampering**	The AGV's will use small friction brakes on each wheel to slow down. Vehicles tend not to know the brake force applied but do know their speed. When the AGV nears the location it needs to stop at the brakes are applied. Loosening the brakes would cause the AGV to not stop in time and could mean the AGV's crashes into things.	Although this is a manual vulnerability, someone who wanted to sabotage the workings of the warehouse could do so using this method with relative ease. For a calliper brake, one would need to loosen the pivot bolt. All AGV's would need to be checked to ensure they are working correctly; this would cause the warehouse function to stop.
Changing the configuration parameters of the AGV	**Tampering**	AGV's usually have adjustable configuration parameters to suit a wide variety of warehouse layouts and customer needs. The AGV's will most likely have some sort of connectivity port to allow for updates and diagnostics. A user could plug in a device and maliciously change the parameters such as the travel speed and the paths that the AGV is allowed to follow. Given that the AGV is also connected to the WiFi, it is possible to connect to the AGV remotely, if the WiFi channel has no privacy or WPA2 encryption protocols.	· Altering the configuration parameters of the AGV could lead to the AGV becoming unaware of where it is within the warehouse. This could lead to the AGV crashing into things causing damage. · The AGV's could be told that when they have dropped off the parcel to rotate on the spot, rather than go to the waiting area within the warehouse. This would essentially create an everlasting job and would eventually lead to no free AGV's and the warehouse function would stop. · The location the AGV waits at when it has no job could be changed. The AGV's could be told to wait in the main aisles and stop each other from completing their jobs.
Warehouse may have WiFi drop out areas	**Denial of Service**	The shelves used to store parcels could block the WiFi signal to the AGV's. There may be areas in the warehouse where the AGV cannot communicate with the command centre.	· The AGV's would not know whether they need to go to the waiting point in the warehouse or if they are required to undertake a new task. They would be unable to contact the command centre to report that they have finished their job, the AGV would therefore remain stationary. · The command centre would also be unaware of which AGV's have finished their task. This could lead to many AGV's becoming stuck in areas of no WIFI and none able to pick up parcels from the reception or drop parcels off at the loading bay.
Fake tasks could be sent to the AGV	**Spoofing**	Because the AGV's are connected over the WiFi network, network packets that are sent to the AGV from the command centre could be collected. These packets could then be replayed or reverse engineering to assign the AGV's new unauthorised tasks.	· The AGV could be given tasks such as hiding delivered parcels in the warehouse which could then be stolen by a member of staff. · The AGV's could be sent a task to take parcels that had not been ordered to the drone loading bay, for example more of higher value parcel could be taken to the loading bay and delivered to a recipient.

Threats to the Stock Database and Related IT Systems

The Stock Database stores the inventory information and whether parcels are in stock and their location within the warehouse. This database is critical in assuring the correct parcels are delivered to the clients. Any changes to the information stored in the database could lead to incorrect parcels being delivered or no parcels being delivered at all. Vulnerabilities found in the stock database are also shared with other components in the delivery system. Figure 8 shows how attacks could gain unauthorised access to the stock database and related IT systems through the access points within the warehouse.

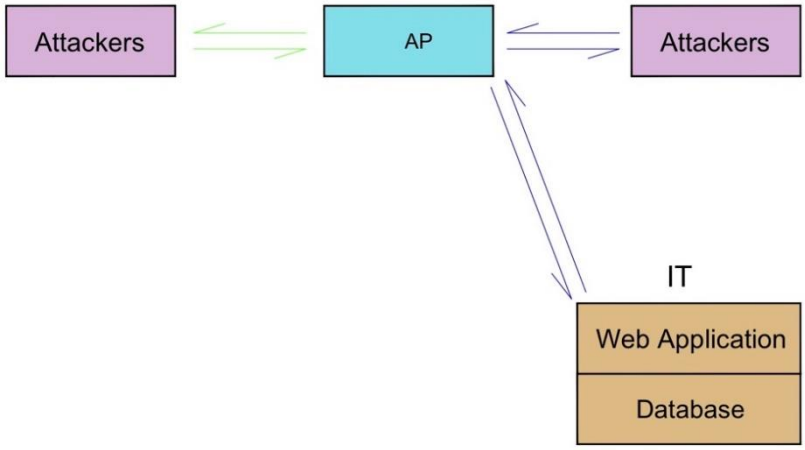


Figure 8: Diagram explaining the process of how the stock database could be accessed by an unauthorised user via the access points within the warehouse.

Vulnerability	Category	Method	Impact
RFID reader and the stock database communicate over the WiFi network	**Tampering**	Requests and responses are transferred across the WiFi networking in the warehouse. An attacker could also send fake requests to the database altering the stock information stored on the database.	· The storage location of high price parcels could be swapped with lower price parcels so the AGV's bring higher priced item to the drone for delivery than what is on the order. · Information on the inventory of stock could be altered with fake stock update requests. This could lead to the command centre believing there is no stock in the whole warehouse and orders could not be fulfilled.

Threats to the Remote Command Centre and Order Database

The remote command centre is the component in the system with the most control over the delivery process. It communicates with the recipients and the drones through the mobile network, the AGV's via the Wifi network and the stock database through a standard high-speed broadband connection. To an attacker the remote command centre is the component of most interest, controlling this grants access to almost all aspects of SHORC's automated delivery system. Given the number of communication channels linked to the command centre, there are many attack vectors available. A diagram of these communication channels is given in figure 9.

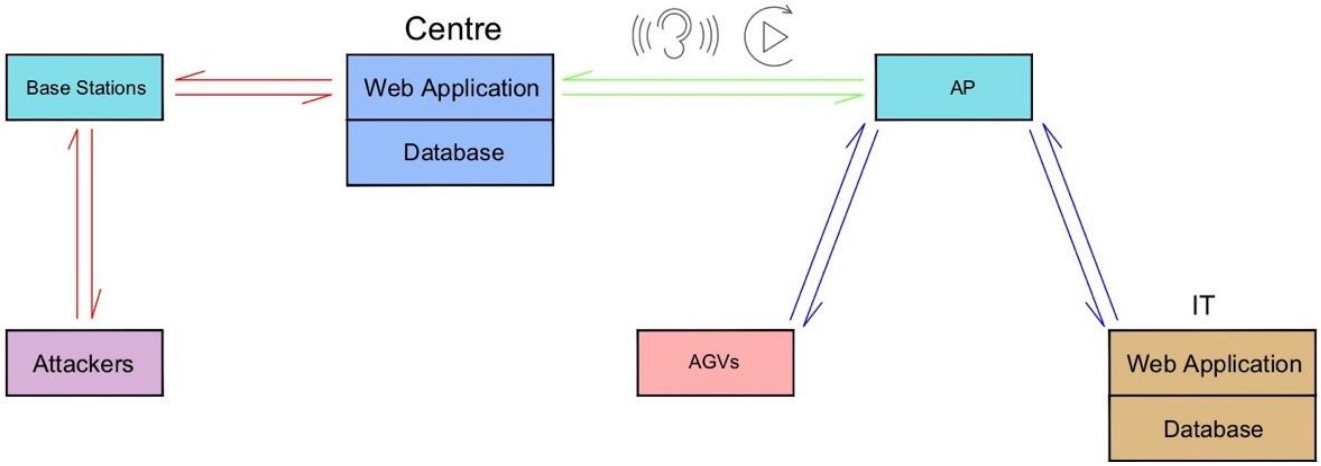


Figure 9: Diagram explaining the process of how the remote command centre could be accessed by an unauthorised user via the access points within the warehouse. In this diagram a replay attack is shown, the attacker is listening to packets transmitted between the command centre and an access point, these packets can then be replayed or reverse engineered to send malicious data to the command centre.

Vulnerability	Category	Method	Impact
Injection payloads could be entered into the order data fields	Multiple depends on the target of the payload. Repudiation, Payload could delete logs. Information Disclosure, payload could leak code used by the centre.	When a user creates an order, the details of this order are sent to the remote delivery centre so that the delivery can be scheduled. The fields of the order could be used to add injection payloads, when the remote delivery centre reads the delivery information the payload is activated.	The Remote Delivery Centre communicates with almost all aspects of the SHORC system. Payloads could be used to reveal information about other deliveries, change the delivery address and increase the number of parcels of each delivery. The number of possible impacts depend on the integrity of other components of the system and how freely the command centre can communicate with the other components.

Vulnerability	Category	Method	Impact
Overflow Attack on the order data fields.	**Elevation of Privileges**	When an order is created, a large quantity of data could be added to one of the order fields. When the remote delivery centre reads the data, the stack buffer will read more data than it can hold and hence an overflow will occur. Exploiting this overflow could allow an attacker to modify internal variables.	When the buffer overflows, data is written onto another buffer re-writing any data held there. The data sent to cause the overflow can contain the next steps as to where the overflow process should go next. The next step could be to add the attacker as an admin on the system. This would allow the attack access to critical components of the SHORC system.
Exploited drones or AGV's could spam the centre with information.	**Denial of Service**	An exploited AGV or Drone could be programmed to spam the centre with data packets. Given the warehouse has multiple drones and AGV's which communicate on separate networks, they could all spam at the same time. The drones work on the mobile network and the AGV's WIFI hence, there would be the bandwidth available to create a distributed denial of service as the Remote delivery centre would be unable to cope with the network traffic.	The Remote Delivery Centre would be put offline, AGV's would be unable to receive tasks and so deliveries would go unfulfilled and parcels would not be collected and stored from the reception. Drones could not be sent recharge requests and so could run out of battery mid-air.
Data on the network between the stock database and the Remote Delivery Centre could be intercepted.	**Spoofing, Information Disclosure, Denial of Service**	The Remote Delivery Centre communicates with the stock database over a standard broadband connection to determine whether parcels are in stock. A user could intercept data packets across this channel and store them. These stored packets could be replayed in a race against the stock database to alter the actions taken by the Remote Delivery Centre.	When the Remote Delivery Centre generates a delivery schedule, it first queries as to whether parcels for the order are in stock. A malicious user could replay a packet that tells the Remote Delivery Centre that the parcel is out of stock for every order. The replayed packet would arrive at the centre first because the stock database would have to query its database before its response is sent back to the centre. This would create a denial of service as no orders would be scheduled for delivery as all parcels would appear out of stock.
Nonofficial updates could but downloaded onto the drones and AGV's	**Spoofing**	Break through the authentication of the Remote Delivery Centre by brute force or SQL injection, then replace the original upgrade package in the database with one that contains malware.	If drones and AGVs are supplied with tampered updates, then gain remote access to them or perform some unexpected behaviour. This might lead to the drone crashing or AGV's targeting warehouse workers. Wrong goods could be delivered etc.

Threats to Drones

The drones are able to have complete autonomy over their own movement as well as be controlled by a remote operator. For this to be the case, the drone communicates over the mobile network with other components such as the GPS satellites, command centre and clients. The amount of data sent to the drone over the mobile network is large and the frequency the drone interacts with other components is high. This makes the drone more vulnerable as there are multiple large attack vectors. Figure 10 shows some possible attack vectors.

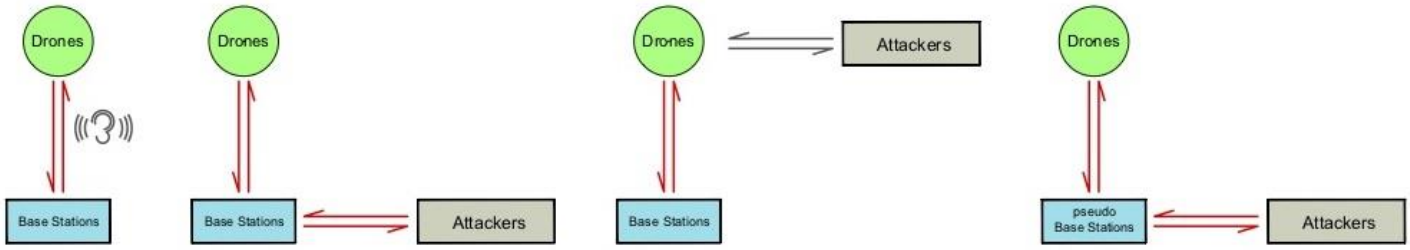


Figure 10: Diagram explaining some of the attack vectors present in the drones used for SHORC's automated delivery system. The left most diagram illustrates that a user could sniff data packets between the drone and a network base station and replay them. The next from the left shows how an attacker could send malicious packets with the IP of the drone through the mobile network. The middle diagram shows that an attack could involve physically tampering with the drone. The diagram on the right illustrates how a pseudo base station could be created to relay malicious information to the drone.

Vulnerability	Category	Method	Impact
Data packets can be collected using traffic analysis tools such as Wireshark.	**Information Disclosure**	Network traffic contains data packets shared between drones and the remote command centre. Through traffic analysis, a vast amount of data can be collected from drones. Data collected includes the drone's IP address, the centres IP address and even sensitive information regarding the delivery and order details.	The IP address and port information of the drones and the remote command centre are published. These could be subject to DoS. The delivery information can also be collected and sold to rival companies in an attempt to gain customers.
The commands and information sent from the Remote Command Centre can be tampered with.	**Tampering**	Attackers can intercept the information transmitted between the drones and the centre. This information can then be modified and re-sent to the drone using network interception tools, such as Charles.	· An attacker could modify the delivery information a drones receives from the centre. The wrong delivery coordinate, address and image, causing the drone to navigate to wherever the hacker wants. · The take-off command from the centre could be modified or intercepted, the drone could be stopped from taking off or giving incorrect take off commands. · The centre's request to inquire about the power status of the drone and corresponding response from the drone could be intercepted. Incorrect responses could be given and the drone will run out of charge, failing to deliver parcels.

Vulnerability	Category	Method	Impact
Unofficial updates could be installed on the drone.	**Tampering**	The drone's software is updated via the mobile internet. An attacker can bind the malicious program to the new software, the malicious program will be installed when drones update the software.	Possible complete control over the drones navigation and movements.
GPS signals can be simulated	**Tampering**	An attacker can use a GPS signal generator to generate a spoofing signal by spoofing the C/A code. An attacker can also adjust the time delay of the received satellite signals. These signals can be amplified and forwarded, this would stop the drone from receiving real satellite signals.	An incorrect GPS signal could crash the drone, or force it to land by making it think it is within the boundaries of a restricted zone.
Intercept the on-board video data stream	**Tampering, Information Disclosure**	An operator can control the drone using the on-board cameras. The video recorded by the cameras is streamed back to the operator over the mobile network. Attackers can intercept and tamper with the on-board video stream using network interception tools.	Disclosing on-board video streams can give attackers information about the drone's routes. Tampering with the on-board video can mislead operators and lead to accidents involving the drone.
The drone receives information from its surroundings.	**Denial of Service**	The centre sends requests to the drone about its power status, the drone responds with its power status. A hacker can launch a DoS attack on a drone using information such as IP, port and battery status from the response given by the drone.	DoS attacks cause the network traffic to become blocked. This cause's communication with the drone to cease or adds in delay between the drone operator and the drone. This would limit the accuracy of drone navigation, possibly causing crashes.
Cameras and other devices used by the drone have vulnerabilities.	**Information Disclosure, Tampering**	Hackers could take control of the drone by taking advantage of discovered flaws in the drone's components. Because the camera for example is connected to the drone, malware could be injected into the video content and used to attack the drone.	· The malware could shut down the drone's components and cause the drone to crash, data stored on the drone could be disclosed. · If a malicious program is injected into the drone using a camera vulnerability, the attacker will gain access to control of the drone, which is awful.

Threats to Clients

Clients are provided with a passcode to open the storage compartment on the drone.	**Spoofing**	Providing clients with a passcode gives an opportunity to create a phishing or spear phishing scam. An email or text could be sent out replicating what is sent by SHORC, but it contains a link directing you to the passcode. This link instead installs malware on the client's device. A spear phishing scheme could also be created, if a hacker has access to delivery information. A fake passcode message could be sent before the real one is sent to a specific client.	Malware could be installed on a client's device, clients would then be wary as to whether the received passcode message is legitimate or not. This would reduce the public's trust in SHORC and automated delivery systems.

Security Requirements

In order to ensure that the SHORC automated delivery system operates normally with protection from vulnerabilities and the impact from exploits contained to a minimum; each component of the system needs to have some sort of security requirements and procedures SHORC should follow.

Requirements for RFID

A way to prevent vulnerabilities involving writing new data to an RFID tag, would be to use RFID tags that are read only. Hence, the information could not be overwritten by a malicious RFID reader. Using tags that have some sort of tamper resistance and basic encryption would stop the sniffing of data stored on the tags, these tags would be more expensive but they would be cheaper than the expensive relating to the delivery of incorrect parcels because of the vulnerability. The more secure tags would not completely stop the exploit but would increase the difficulty for an attacker. Furthermore, reducing the range of the RFID tag would mean that an attacker would need to be in close contact with the tags to exploit it. If possible each different RFID tag should be set a different induction frequency, this would limit the impact of a possible jamming attack. The requirements for RFID tags are set out in figure 11.

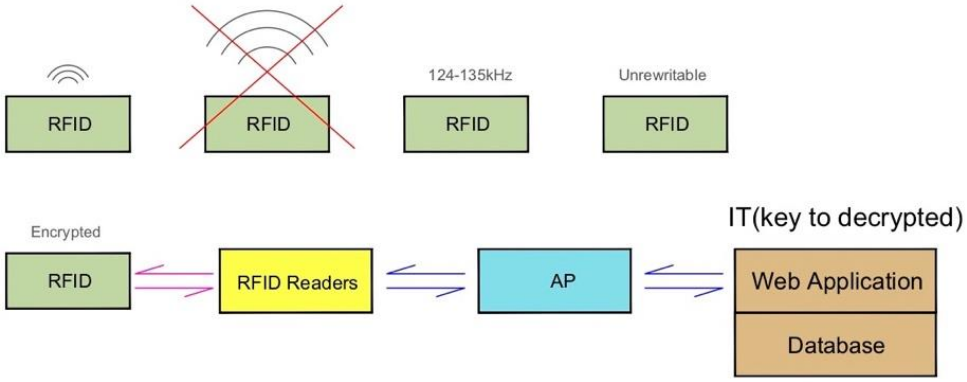


Figure 11: Diagram illustrating some of the requirements for more secure RFID tags. The top row show that the RFID's should have a short induction range, a wide range of possible induction frequencies and should be read only. The bottom row shows how encrypted data stored on the RFID would be accessed within the SHORC system.

Requirements for Access Points

To reduce the possibility of WiFi-connected components such as the AGV's within the warehouse from being hacked; other external devices such as staff phones should not be allowed to connect to the warehouse WiFi. The WiFi network should employ some sort of encryption through WPA2 or WEP among other encryption methods, this would limit the ability for a malicious network user to collect and understand network packets. The switches used to connect the access points and the remote command centre should be supervised. Switches can avoid illegal devices from accessing the network by the means of MAC address authentication and port isolation. These measures can also be used in access ports.

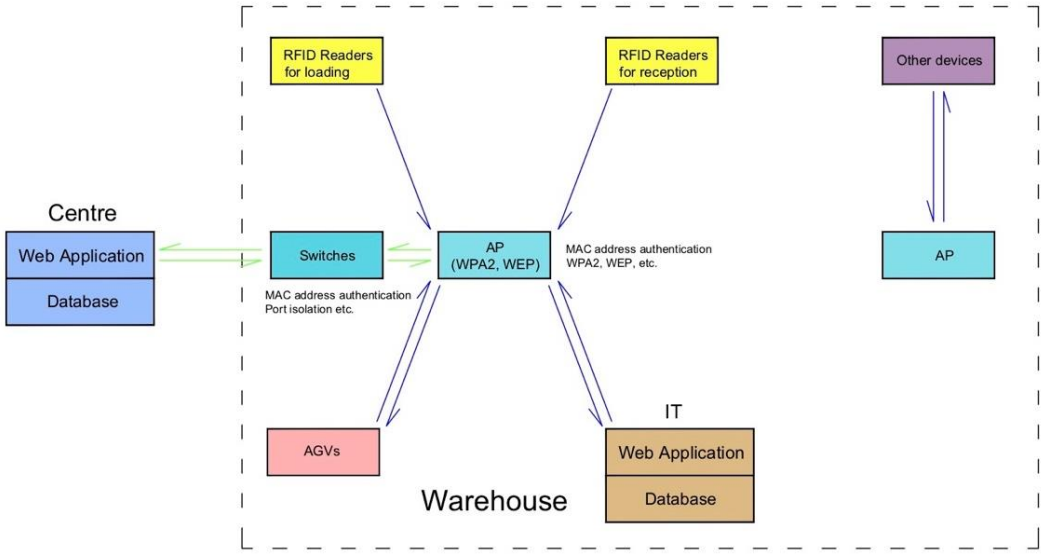


Figure 12: Diagram detailing how the access points could be secured to reduce the possibility of vulnerabilities from being exploited.

Requirements for the Stock Database and Related IT Systems

The stock database needs to have protection measures against SQL injection attacks, data sent by the RFID readers and queries from the remote command centre may include injection payloads. Additionally, when a user wants to login to the IT web application, a limit should be placed on the number of incorrect login attempts to avoid brute force by attackers. The administrator's login information should be strong and have complex passwords. When an admin modifies information in the stock database, at least two or more people need to confirm this action before the modification is made, this avoids theft by staff if storage locations were changed incorrectly.

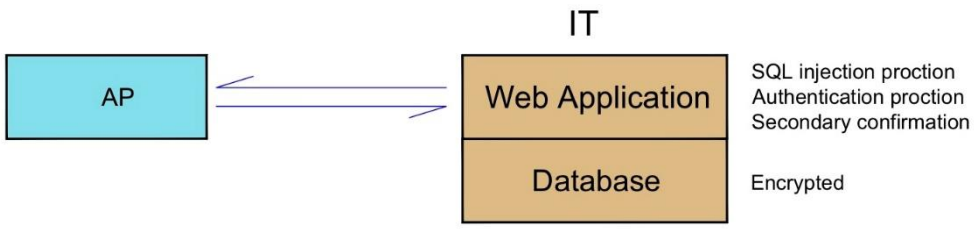


Figure 13: Diagram detailing how the stock database and related IT could be secured to reduce the possibility of vulnerabilities from being exploited.

Requirements for AGV's

An attack on an AGV's configuration settings, may cause it to act in ways that could harm staffs or damage the facilities in the warehouse. One way to prevent this, is that the areas in which the AGV's work in should be clearly defined. The access points used by the AGV's should be separated from the communication modules, ensuring that even if an AGV is attacked, it will not cause as much damage that the attacker would expect. Furthermore, guidelines as shown in figure 14, can be laid down in the warehouse and AGV's are set to only follow the path of these lines in all scenarios. If AGVs is attacked, as long as members of do not walk onto these lines, then the AGV's will not be able to cause harm to members of staff.

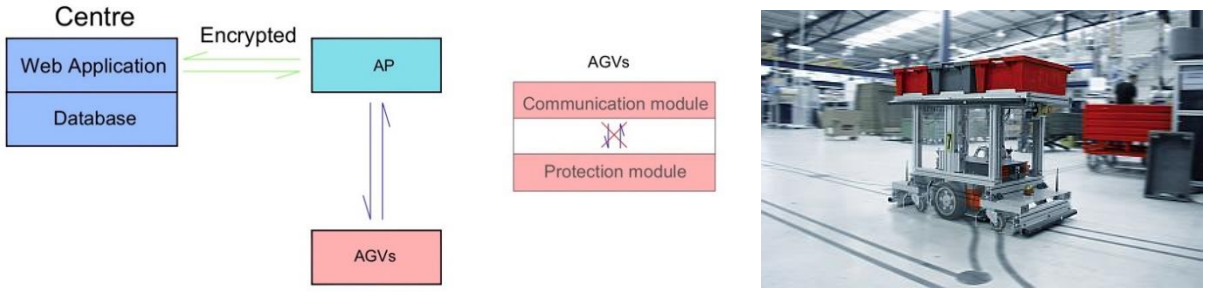


Figure 14: The diagram on the left details how the AGV's could be secured using encrypted communications between the AGV and the remote command centre to reduce the possibility of malicious users from collecting network packets. The diagram in the middle shows how the AGV's should be disconnected from the main warehouse network using protection modules. The picture on the right illustrates how guidelines could be marked onto the warehouse floor which guide the AGV's where to go.

Requirements for the Remote Command Centre

Compared with the Stock Database and IT, the Remote Command Centre interfaces with clients, drones and AGVs. If the Centre is attacked, it will cause not only loss of items but also potential risks such as information leakage. In addition to protection from SQL injection attack vectors, authentication protection and secondary account confirmation will be required to further improve the remote command centres security and ensure users are legitimate, this is shown in figure 15. For example, the server used by the command centre must be able to withstand DOS attacks by setting reverse proxy and firewalls etc. Passwords sent by the command centre to customers should be randomly generated to prevent attackers from easily cracking them and gaining access to parcels.

In addition, the command centre should monitor the weather at all times. This is to avoid sending drones to places with bad weather or request drones back if the weather gets worse. Bad weather could cause damage to the drones and stored parcels. User information in the database; such as account passwords, purchase history and credit card information should be securely encrypted. This avoids in the case of a data breach that the hacker can read the data stored. In the case of data breaches or data loss, information needs to be backed up. This is shown in figure 16.

When the command centre downloads software update files from the drone manufacturer, it should make sure that the files are not embedded with malware such as trojans by checking their MD5 and hash.

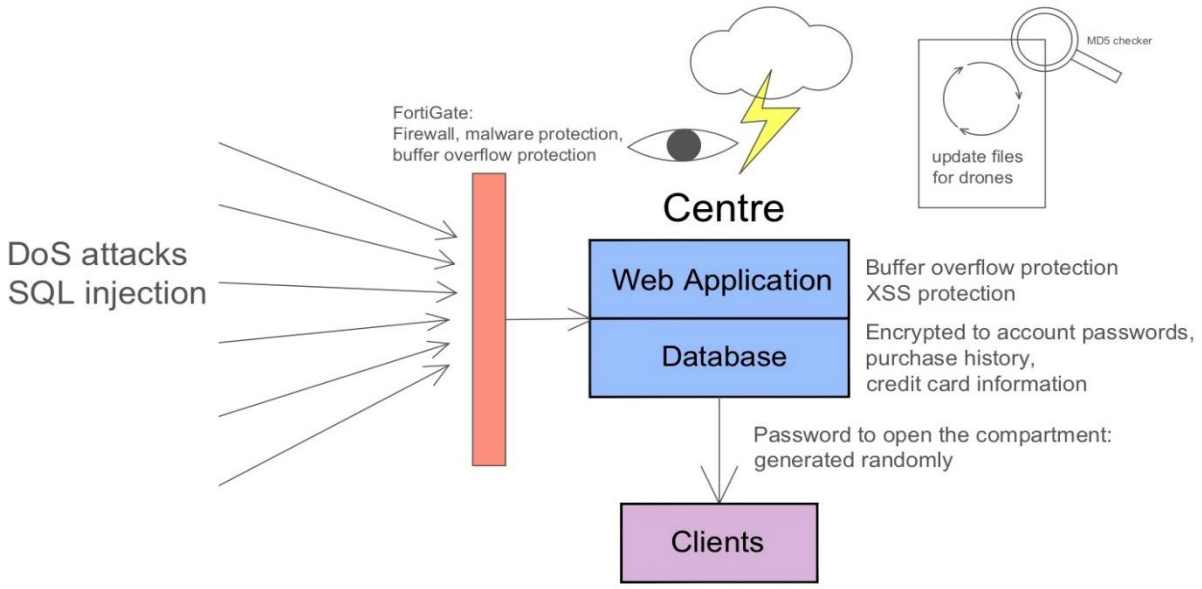


Figure 15: The diagram illustrates the extra authentication and protection techniques that should be employed by the remote command centre to protect the centre from exploitable vulnerabilities.

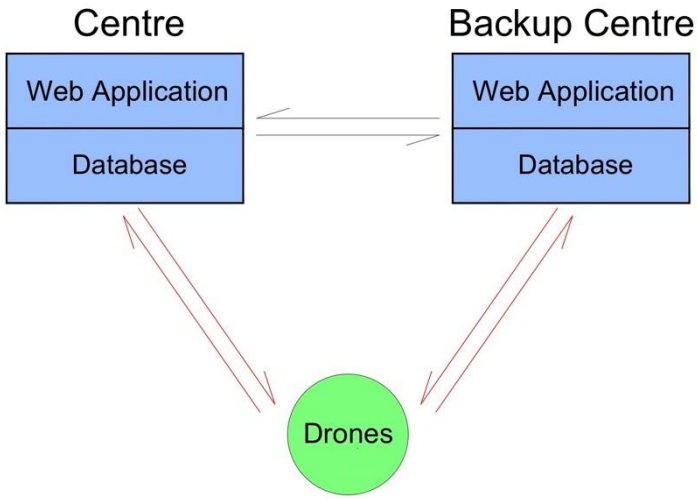


Figure 16: Diagram detailing how the data stored in the order database could be backed up to an outsourced backup centre.

Requirements for Drones

The drones locate their coordinate and destination coordinate according to GPS, the reliability of the GPS information can be guaranteed by verifying the information with supporting GPS satellites. Similarly, communications between the drone and the command centre needs to have backup communication channels to allow the command centre to send weather information and allow the operator to control the drone even if one channel fails. This process is shown in figure 17.

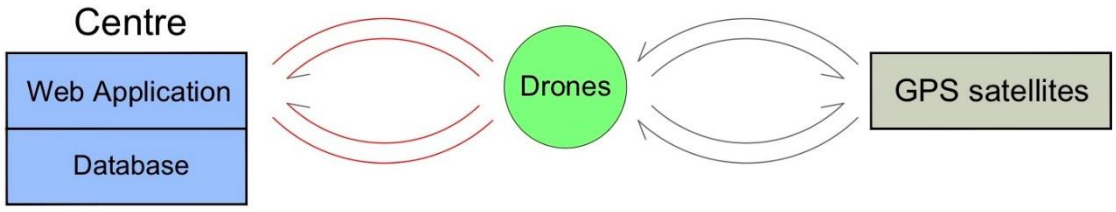
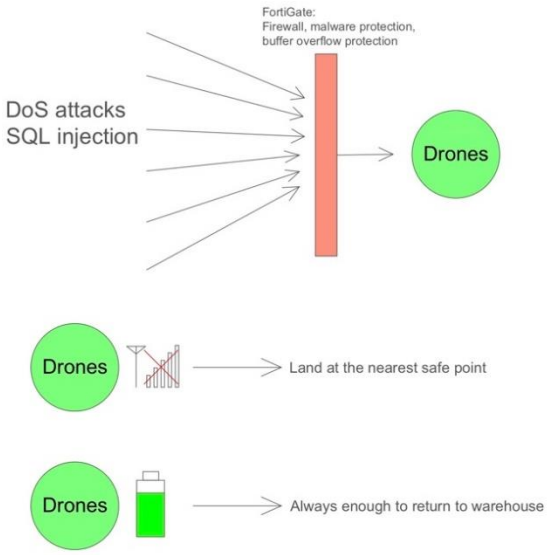


Figure 17: Diagram illustrating how multiple network channels could be used to ensure smooth communication between the drone and connected system components.

The drones should have firewalls and malware protection that can prevent attackers from stealing information like the passcode, items and destination from the drone. The drone should have fail-safe mechanisms to ensure that it can land at a safe point if connection to the mobile internet or GPS signal is lost for a long period of time. Also, the remaining battery should always be enough to allow the drone to return to warehouse. For example, when the drone is delivering items; if the battery is close to the point that it cannot provide enough power to return to the warehouse it shall return to the warehouse immediately, even if the delivery has not been completed.



Furthermore, the storage compartment of the drone must be strong enough to prevent an attacker from violently damaging and stealing the parcels stored inside. For safety reasons, if the compartment of the drone has been opened, the compartment must be empty when the drone returns to prevent someone from putting harmful things like a bomb in it.

Requirements for Clients

Clients should keep a safe distance from the drone until the propeller has stopped, and once the customers has picked up their items they must make sure nothing is left in the compartment and close the door securely. These requirements are shown in figure 18. Customers should also be aware that if the parcel has not been collected from the drone within 2 minutes of the drone landing that it will return back to the warehouse, this is to stop other people from stealing the drone or its contents. To limit the potential for a phishing scam relating to the supplied passcodes customers should log into the correct website or APP to ensure that the passcode received is official.

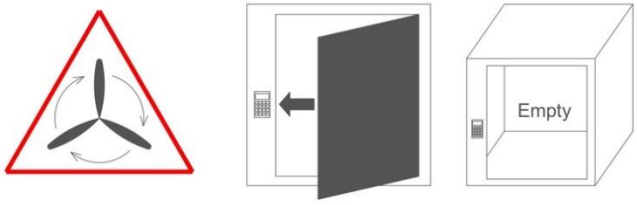


Figure 18: Pictures representing the requirements for how a client should interact with a drone, the image on the left shows that clients should stay away from the drone whilst the rotors are still spinning, the next two show that the parcel compartment should be left empty.

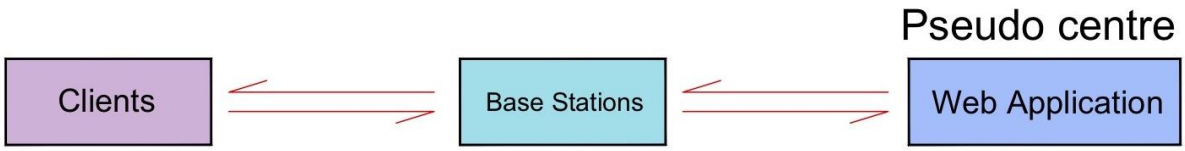


Figure 19: Diagram representing how a phishing scam could send false and malicious information to the clients.

Major Challenges to Privacy

The SHARC delivery system has three main areas that contain privacy concerns. The first being that the drone will be flying over people's houses whilst filming using a 360 degree camera. The sensitive data surrounding the nature of the parcels, what they contain along with who they are being delivered to and finally the data kept about users in the Remote Delivery Centre database.

Drones Invading Personal Privacy

In a study by Pew Research Centre in 2018, 54% of the public thought that drones should be banned from flying near homes. The major concern being that drones could take pictures or videos of people's houses and this is an invasion of their privacy. Currently, there is no fixed legalisation as to what a drone can and can't film, but interestingly satellites have been able to picture people's homes in a similar manner for years. However, drones are far more controllable and are able to obtain up to date pictures of specific areas with far less hassle. For deliveries to be made by SHORC with drones, the drones will have to be able to fly over people's homes.

Therefore, a method to combat this privacy concern is to limit the areas in which the drone can film. The drone is supplied with the coordinates of the delivery landing site, the camera should only be used when the drone is within close proximity to the landing site. The camera can then be used to identify whether what the drone sees matches the supplied landing site picture, this would stop the drone from filming over the full duration of the delivery flights. This method would reduce privacy concerns as the camera films only in critical situations such as landing and taking off.

It is expected that the drone contains other methods of navigation for cases such as flying during the night or fog where the cameras would not work. Radar is one such method and can be used to navigate the drone correctly in both automated or operator controlled modes when the camera is switch off, without hindering the drone's ability to deliver parcels.

Data Stored on the Drones

Most drones have the ability to store flight information such as the route taken or video filmed. This data must be stored securely within the drone; otherwise when the drone lands at the delivery location, a malicious user could take the storage medium and access the video or routes taken by the drone. The data stored must therefore be encrypted with a secure scheme. Given that this data won't be transmitted or required in time critical processes, the strength of encryption can be high.

A Malicious Staff Member could determine what the Parcel Contains

Each parcel has an RFID tag attached, before the parcel is loaded onto the drone the RFID is interrogated by a member of staff at the loading bay. A staff member could determine what the parcel contains and depending on the nature of the parcel they could blackmail the recipient about it.

RFID's should not store any information about the parcels contents, they should only store an ID which is then matched against the ID's in the order and stock database. Furthermore, the parcels to be delivered should be stored in discreet packaging, similar to Amazons delivery boxes, this would stop staff in the loading bay from determining the nature of the parcels. The need for a delivery address or recipients name on the packaging could be optional. For most deliveries the only stage in the delivery process is the drone, the drone knows the delivery location and only the true recipient can legitimately open the storage compartment gaining access to the parcel. This would further reduce privacy concerns about staff finding out where parcels are going and who is receiving them.

A Malicious User could Scan the RFID and determine what the Parcel Contains

When the drone lands for delivery or if shot down, a user could interrogate the RFID on the parcel stored within the drone and find out what the parcel is and whether it is worth stealing. The storage compartment of the drone should be made out of a secure material which if possible creates a Faraday Cage. The Faraday Cage would stop unauthorised users from interrogating the RFID's inside. The drone should also have a method of alerting the Remote Delivery Centre and give out an audible alarm if there has been unauthorised access to the parcel storage area.

SHORC Operates within the UK and is bound by European Data Laws

The delivery drones and Remote Delivery Centre store personal data. The way the data is stored, used and modified must satisfy GDPR rules. GDPR is designed to give users greater access to their data, so they can see what companies are storing, with the aim of alleviating privacy concerns as well as defining strict guidelines to ensure data is kept securely. Some examples of GDPR are that if any data is breached then authorities must be told within 72 hours of whose data has been breached. Users can also ask for their data to be erased from databases if it is no longer necessary for the purpose it was collected for. Data about users orders could be deleted a short time after the delivery has been successfully made, this would limit the amount of personal data stored and reduce privacy concerns. The data stored could also be encrypted to limit the amount of personal data leaked in the case of data breaches.

Major Challenges to Safety

The SHORC delivery system faces three major safety challenges. In the SHORC delivery system, there are three main components where safety issues are most likely to arise, the drones, AVG's and the parcels. On one hand, the damage caused by drones and the threat to public safety is mainly caused by the improper handling of unexpected situations during the drone's flight. On the other hand, due to errors in the AVG system, stock and the contents of the warehouse may be damaged and staff incidents may occur. There is currently no relative regulation law on drones at present, whether the parcels delivered by drones will pose a threat to the government and citizens is an issue worthy of attention.

Safety Concerns related to Drones

In the process of carrying out delivery tasks, drones will encounter many unpredictable external factors such as weather; electrical interference, mobile internet signal strength and aviation traffic. There is also the possibility that the drone might be attacked when landing or taking off at low distance from the ground. The drone may have crashed during transport due to lack of power, signal or bad weather. Any drone crash poses a safety risk to the public as there is a possibility that a crashing drone might hit a member of the public. Furthermore, areas of high aviation traffic density should be off limits to the drone, drones and civil aviation traffic mixing in the same airspace is a critical security concern.

Safety Concerns related to Parcels

At present, all kinds of mature forms of logistics, such as airplane, truck and ferry have strict laws and regulations. But there is no regulation for the use of drones in logistics. It is doubtful that all parcels being delivered by drones are in compliance with the law. Illegal goods, such as explosives, pose a great threat to governments and the general public. There is no denying that the safety of drones also directly effects the safety of parcels, with the high rate of damage to drones leading to high rates of damage to parcels.

Safety Concerns related to AGV's

AVG's may cause accidents due to system errors, these will create a large financial loss and personal safety threats to the SHORC delivery system. The AVG's are the main means of transportation in the warehouse, damaging the AVG's camera or sensors may lead to the failure of the AVG to correctly identify any obstacles. This would result in a collision with obstacles that could be containers, staff or other AVG's.

Solutions to the Safety Concerns

Considering the problems posed by drones mentioned above, the first solution is that the drones should make reasonable scheduling plans at different power levels, so as to not crash if the drone has insufficient power. For example, after the drone receives the delivery address; it should first calculate whether the power remaining is enough to complete the delivery, if not, it should send a signal to inform the center to arrange charging. Or when the drone needs to deliver multiple goods to different destinations during the same flight, it should calculate in real time whether the remaining power is enough to deliver the next goods in the schedule and return back to base. If not, it should pause the delivery schedule and return to the base, recharge and then continue the schedule.

In operator assisted mode, if the mobile internet signal is poor, the operator should take the initiative to release control of the drone. The drone will automatically switch to automated mode flight and continue the delivery. Drones should also not be allowed to take off in bad weather, due to the current capability of the drone to combat adverse environments is inadequate. To prevent drones from being vandalized during takeoff and landing, they should use their own cameras to transmit video data and alert the command centre in real time if the drone is in danger. An alarm could also be used to deter vandals. In addition, as the number of drones increases, the navigation routes used by the drones is a problem that the government needs to pay more attention to in order to avoid the occurrence of drone collisions or affecting the flight paths of civil aircraft.

In order to solve the problem of parcel legality, law enforcement departments need to issue supervision laws on drone delivery. It is also possible to install scanners inside the drones to ensure the goods stored in the compartment are legitimate. To reduce the damage rate of parcels, the first step is to reduce the damage rate of drones, the measures mentioned above can be taken to prevent the damage of drones.

To reduce the damage caused by collisions caused by system errors or cameras and sensors abnormalities, the AGV's driving speed could be lowered so as not to lead to serious accidents. The AVG’s should be inspected regularly, and staff should pay attention to the status of the AGV’s through monitors during warehouse operation. After an accident, it is also important to send out an alert to inform the staff to deal with quickly and source the cause of the accident encase the threat exists to multiple AGV’s.