Cyber Security in BA

Security is paramount in the aviation industry, there are approximately 717 airports (Commercial, Private and Military) in the mainland UK alone. At least 40 of those are international commercial ones. The security for these airports is undeniably important.

Following the data breach at British Airways (BA), there needs to be a revitalization in the security. Regarding the hardware, software and physical based protection from attacks and malicious activity, thus insuring the prevention of more data-loss and nullifying the risk of a successful attack. Within this document, each of the current methods implemented will be revised to identify security weaknesses.

Current Implemented System in BA

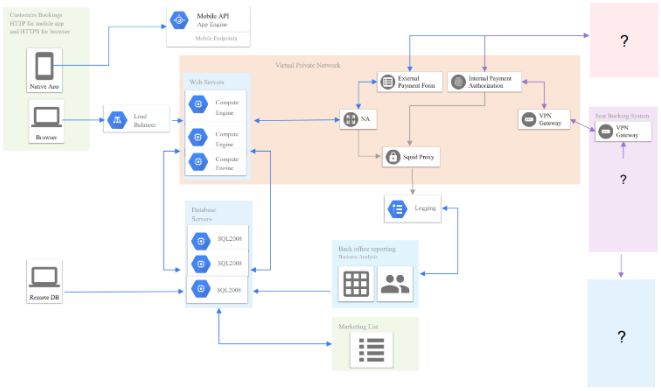

*Figure 1*CMP3745M Assignment 1*

Regarding the mobile API currently exhibited in the current system see fig 1*, there can be a varying degree of security parameters set in place by the app itself. For example, depending on the security settings the API could have Basic Base 64 Authorization (username & password) however the information is sent on every request and it is stored locally on the device. One suggested upgrade to this, would be to use bearer authentication. Needing to write an endpoint and an appropriate format for the client to understand is a mild complication but necessary as it's much more secure as you have complete control over token (tokenization is essentially encryption of the password and username) usage and state.

To distribute the load across all of the different web servers it uses a load balancer, there is nothing inherently wrong with this practice as the security isn't compromised as it just ensures the traffic is shared. The web servers are held in a closed VPN (Virtual Private Network) this encrypts the connection over the internet, the load barer must be using a token or a unique identification procedure to gain access to this network.

Within this VPN it consists of the External Payment form to ensure all of the data in the form is encrypted within the VPN as with the Internal Payment form the Web servers aren't behind any other form of privacy or encryption other than the VPN. The database server connected to the web servers isn't secure within the VPN however the main form of connection received would be from the remote DB probably using one step verification.

Squid Proxy isn't security based it's a more ease of access and response time based proxy server it's use is caching webpages and frequently viewed content to allow for faster loading times. There are a few security concerns in the current versions (2018) of Squid Caching. One of the most prevalent security concerns would be the ability to gain user based access with a DoS (Denial-of-Service) Exec Code Overflow based attack. It allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long WCCP packet

The back office reporting and business analysis logs all information with the squid proxy, and only sends information to the database servers in order to securely store the information. Marketing list

purely communicates with the database servers and has no access to the web servers directly meaning attacks are far less prevalent.

Overview of the Current System

There is one VPN containing both the web servers and all of the payment forms, it even includes the squid proxy connecting to the logging for the back office reporting. There is a separate VPN for the seat booking system, however the chain between this could be interrupted. The Database Servers are not secure in their own network as they are susceptible to the Remote DB.

Main Security Concerns and Solutions to the Already Existing System

First and foremost one of the largest concerns would be that the Web Servers are contained within the same VPN as the payment forms and the authentication, this means with basic access to the VPN the attacker can access information from the entire database and all of the payment forms. As the Database servers are held without a VPN surrounding them they are free to access from the VPN once the attack has found a vulnerability.

Physical security could be huge issue here too, none of the workstations have any sort of protection on them from attacks. According to figure 1, there are no firewalls internal or external implemented into any of the system. There is a distinct lack of ACL's and any sort of incoming traffic mitigation.

Mitigation

Similarly there are 7 main factors when designing a network (Norris & Pretty, n.d.), these are as follows; User needs, Cost, Performance, Reliability, Availability, Expandability and Manageability. This is important to note, as the changes suggested further on in this document could be seen as to adhering to these principles. Keeping an ability to expand while keeping the core of the network intact. If the security of the network is compromised the damage needs to be minimal, so disallowing any access into any neighbouring system would be important. One of the key parts to keeping a cyber-security system relevant is updating both the software and hardware, keeping the staff trained and updated with current methods of cyber-attack is vital. Public areas often have heating, ventilation and air conditioning controls, access control devices, CCTV and passenger screening equipment.

It may be possible for passengers to gain control of these systems without the physical intervention, doing this would be relatively easy and could lead to much more significant problems like the metal detectors not working properly or even disabling CCTV to path the way to a much more sinister and physically devastating attack. Making sure all of the airports network are secure is very important as they're an international point of contact.

Security Modules

Biba Model widely addresses the issue of integrity; this is characterized by three main goals. The data is protected from modification by unauthorized access, it is also internally and externally consistent. This specific module uses similar to the BLP model, the no read-up rule and the no write-down rule however the Biba module also has the Invocation Property.

Chinese Wall Model is dynamically changing access permissions, it makes so there is no conflict of data with the data they have previously accessed and the data they are attempting to access. This tries to ensure only legitimate changes make take place. Primarily used to avoid conflicts of interest.

Harrison-Ruzo-Ullman based on generic rights and finite set of commands. Naps the subjects, objects and access rights to an access matrix. All configuration is defined as a table or matrix S, O and P.

Bell-LaPadula Model is a state machine model that deals with the preservation of confidentially and only confidentiality. This uses a multi-level with three main rules, Simple security rule this is a no read-up rule. The Star Property Rule, using the no write down method.

Clark-Wilson Model is an issue for integrity and is used to control the subjects' access to an object. It deals with three integrity goals, authentication prevents unauthorized users from making modifications, and it also prevents the authorized users from making improper modifications. It maintains internal and external consistency through well-formed transactions.

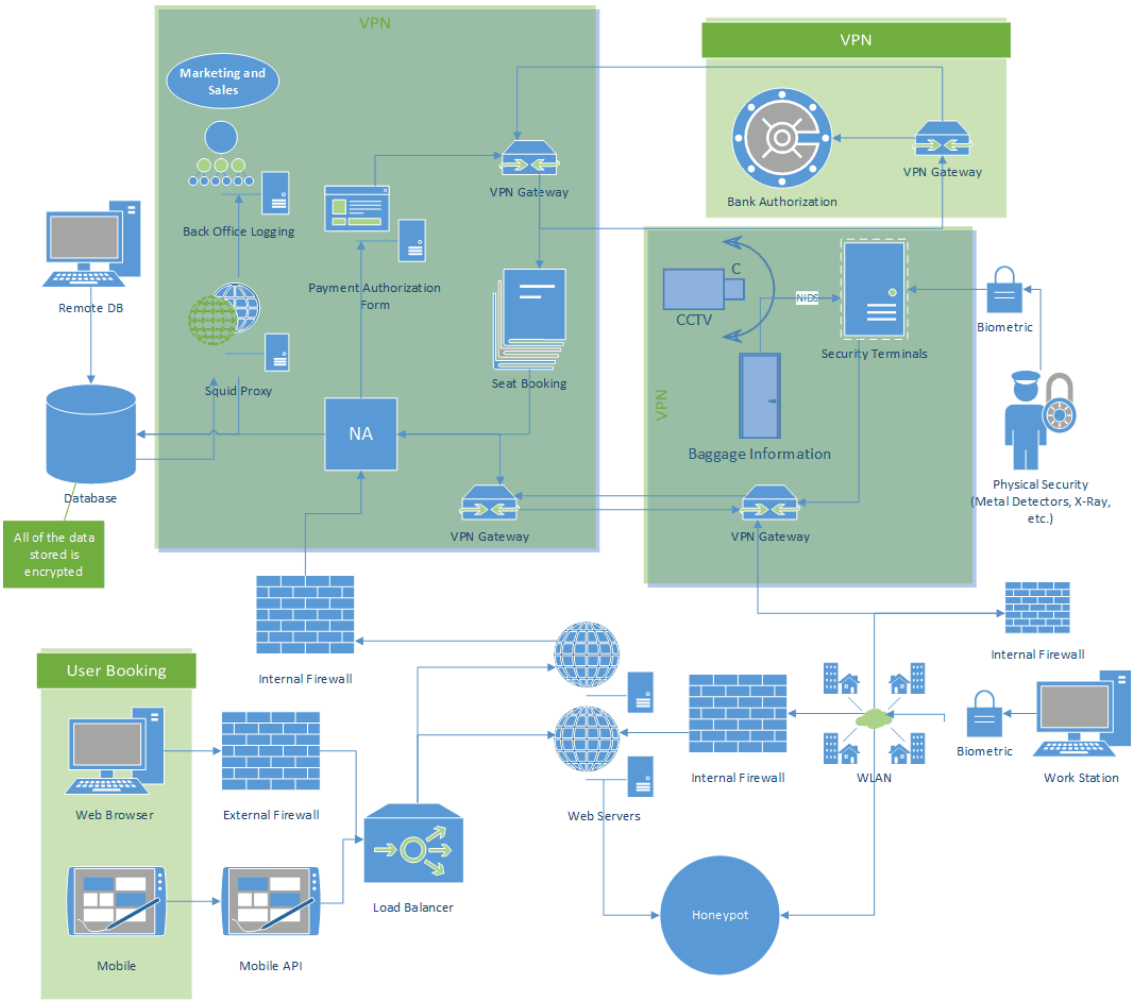

Figure 2

Suggested System

This is the intended new system, each of these design choices has been made taking into account the 7 factors of networking. The cost for this system would be huge but for an airport no cost is too much for security as it's an international pivotal point. Starting from the beginning from an attacking perspective, there will be two separate VPN's, essentially acting as two separate intranets however sharing the same database (purely for convenience). The database being used would be using the Clark-Wilson Module that is used in many military practices due to the security of data and data only being accessibly to the right parties. Having two separate VPN's means if someone the attack gains the access key they wouldn't be allowed free roam over everything in the airport. There are two main means of attack, physical cyber (an attacker on a workstation within the airport), the prevention tactic

I have used for this is loading the computers with a HIDS, and once the intrusion is detected the WLAN would have means of disconnecting and thus isolating the problem. Each member of staff must be using a biometric method of verification to access the WLAN, if this is bypassed the internal firewall would only be allowing certain ports to be open at one point, however a honeytrap would be active separately. Advertising it's very open ports, hoping to catch the intruder before they can do damage. If the intruder manages to get through the internal firewall, they will have access to the Web Servers.

I have chosen not to place these behind a VPN and essentially use them as a DMZ allowing a better understanding of the traffic on the servers and limiting the updates. Using the R1 config to packet trace on the servers, if malicious activity is detected inside the network, the Database would be so far out of reach the chance of loss of data before a shut down or prevention would be minimal.

Coming from the customer perspective, over-flooding the servers would be a low likelihood as the multi-load balancer in cloud (S & Babu, November 4th, 2018) will equalize all traffic and the ACL written in the load balancer will mean once there have been too many bad requests, the IP is timed out for 5 minutes. The secure API security on the mobile would include SSL and API user registration with strong password protection. Adopting a security mechanism between API and the backend (Tang, et al., 2015 12th International Conference).

The internal firewall connecting to the secure VPN containing the non-physical information such as the payment forms would be the only way into the secure network. The only other backend route would be the second internal firewall connecting the CCTV to the work stations. Within the VPN would be the important internal networking items such as the squid proxy connecting to both the database and the marketing. Speeding up all of the information needed from the DB in reference to sales. Payment authorization will be passed along a VPN gateway into an external VPN of the customer's bank to ensure the funds are available. Once conformation is sent back, it goes to the seat booking to reserve the seats available then storing in the DB.

The information in the DB will only be available to the work stations after request and through two VPNS. The purpose of having two separate VPN's is if there is access with malicious intent the damage would be contained to the immediate vicinity rather than that of the whole intranet. The purpose of all of this is to mitigate the issues of both a physical and cyber-attack, with the view of extending the system as needed.

Conclusion of New System Compared to Old System

The new system proposed is vital as it protects the airport from both a physical and cyber-attack in more ways than one. Using the web servers as a DMZ could potentially lead to more access granted to this service and disrupt the servers however with sufficient load bearing this could be mitigated. The VPN with payment would be using L2TP and IPSec, combining both the protocols would be ideal as it provides encryption throughout the process of transmitting data. However the other VPN would be using PPTP as it's widely used. The bagging system would be using a NIDS system to look through the packets being delivered by the network and ensuring nothing malicious is happening. Enabling a secure connection to the baggage information. The encryption method transmitting to and from the database would be AES-256 however other encryptions would either be AES-192 or AES-128 depending on the severity of information and frequency of use. (Higher frequency using less encryption, with the exception of everything connected to the DB and the Payment forms).

References

Anon., n.d. *CVE Security Vulnerabilities,* s.l.: https://www.cvedetails.com/vulnerability-list/vendor_id-9950/product_id-17766/Squid-cache-Squid.html.

Cadee, M. & Willemsen, B., 2015. Extending the airport boundary: Connecting physical security and cybersecurity. In: *Journal of Airport Management.* s.l.:s.n., pp. 232-239.

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. & Phares, B. M., December 2013. CYBER SECURITY FOR AIRPORTS. In: *ational Journal for Traffic and Transport Engineerin.* s.l.:s.n., pp. 365 - 376.

Koch, T. et al., 2017. *Model-based airport security analysis in case of blackouts or cyber-attacks.* s.l., IEEE Computer Society.

Norris, M. & Pretty, S., n.d. The Basics of Network Design. In: *Designing the Total Area Network: Intranets, VPNs and Enterprise Networks Explained.* 1999: s.n., p. 25–50.

Research and Markets, 2017. *2017, Two Day Cyber Security for Airports Summit.* Singapore, s.n.

S, S. & Babu, K. R. R., November 4th, 2018. *Synchronized Multi-Load Balancer with Fault Tolerance in Cloud,* s.l.: s.n.

Tang, L., Ouyang, L. & Tsai, W.-T., 2015 12th International Conference. *Multi-factor web API security for securing Mobile Cloud.* s.l., s.n.

Appendix

No Read-Up – This is the simple notion that the authorization you have can only access your tier of data. For example if there are three tiers and you only have the authorization for the middle tierm, you can't look at data for the upper tier but you can read all the data below.

No Write-Down – This stops the ability for data being shared to a lower authorization area or database. Essentially destroying the security levels.

Invocation Property – Simply states a process from below the required access cannot request a higher access, may only communicate with subjects at an equal or lower level of authorization.

1 Policies and Procedures in 2 Cyber-Security

A cyber-attack could be either physical activation of a piece of software or a hacker maliciously getting into a network through an open port via wireless signals. Cyber-attacks widely incorporate any attack on the intranet or closed confidential network. (Kaiser & Mejia-Kaiser, Vol. 64, Issue 2 (2015))

3 Summary

Airports are a pivotal point of contact and as such are under direct threat from an ever increasing and potent cyber-attack force. Aircrafts themselves are never connected to an external network to minimalize safety risks. The airport itself is under threat from cyber-attacks, both physical and wireless. All employees should adhere to the principles laid out, as should all of the cyber procedures taking place.

4 Introduction

The problem with airports is the threat of data breaching, the reason for this report is to try and address what both the staff and hardware could to secure the airport in terms of cyber-security. The increasing threat of cyber-attacks in airports specifically could cause a huge loss of information and make a pathway to a devastating physical attack. It's almost impossible to completely eliminate all risk however this report will look at mitigating most risks in an affordable and convenient manner using the Clark-Wilson model as a basis for internal security.

5 Policies and Procedures

6 Staff Policies

Mitigating the risks from cyber security isn't purely down to the hardware or software (firewalls, honeypots, WLAN, VPN's etc.) it is also largely part on the staff and how they deal with the information being given to them. Keeping confidential data in an airport is extremely important, some examples of these are:

- Financial Information
- Customer Data (Address, Name, Seating Information, Baggage Information)
- Flight Information
- Employee lists

All employees are obligated not to disclose any of this information and protect all of this data. Within this report the method of avoiding security breaches will be highlighted. Protecting personal devices, if an employee is using their own digital devices to access network emails they introduce a security risk to the network and database. Here are some mitigations to use for personal devices;

- Keeping all devices strong password protected
- Maintaining a complete antivirus and antimalware software
- Only logging in through secure and private networks.

Not just personal devices have security issues, the work stations in the WLAN have a margin for human error. A couple of ways to mitigate this is to not access personal emails on the workstations and when not using the terminals don't leave them unlocked at any point.

7 Physical/Cyber Procedures

The physical aspects of security includes but is not exclusive to internal routers and internal dedicated firewalls. Using biometrics to secure the workstations is a form of physical security. In the routers, using an 'R1(config)# login block-for' would be beneficial as this would shutdown the login attempts if tried too many times in a period of time. This would be logging all of the attempts to review if it was a poor connection or something closer to a DoS attack. Firewalls would be installed at the exiting points of the network, this would permitting only necessary traffic enforcing the access control policies. Using the Zone-Based Firewall (Cheswick, Bellovin, & Rubin, 2003) would outweigh the limitations, as there is no authentication support inherently however the biometric access on the WLAN would mitigate the unauthorized access. This would also grant

greater visibility over the incoming packets. Creating a layer defence would be best in the airport scenario as mitigating the information received from the attack would be the best course of action. Each of the work stations would be fitted with a HIDS system, to enable visibility into encrypted packets.

Including a honeypot into the WLAN network would entrap any would be attackers as they would be drawn to this goldmine of fake information of data and power. Ultimately thwarting any attempt made to intrude into the network. The database itself would be encrypted and all of the physical points of contact (baggage, CCTV, Metal Detectors) would be on a separate VPN compared to that of the processing systems, trying to minimalize damage if access is gained to either of the two networks. Using AES 256, would hopefully mean no decryption from the database would be viable. The only method of attack could be that of a social engineering standpoint.

Following the fitting of the new security system, (Gopalakrishnan, Govindarasu, Jacobson, & Phares, 2013) reviewing the security of the network would be important Vulnerability scanning would be an important step to take. Reviewing the network traffic every period of 3 months would ensure the understanding of the networks communications.

8 The Law

Adhering to the policies set out in this report is paramount as it not only policy but its law. The Data Protection Act of 98 means only necessary data should be stored and should be kept up to date. However there is a lacking in Security Legislation, there are no defined principles of security. (Gordon, 2016) It's a grey area so to speak. In aviation there are three principally different areas (Kaiser & Mejia-Kaiser, Vol. 64, Issue 2 (2015)), only one of these is non-safety relevant infrastructure. None of the aircraft should be interconnected with external networks, the only point of contact for the aircraft would be the ATM (Air Traffic Management). This would avoid the threat for aviation to cyber security. This is the critical point of contact for the safety concerns of the aircraft.

9 References

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet security: repelling the wily hacker.* Boston, Mass.; London: Addison-Wesley.

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. W., & Phares, B. M. (2013). CYBER SECURITY FOR AIRPORTS. *International Journal for Traffic & Transport Engineering*, 365-377.

Gordon, J. (2016). *Like a Bad Neighbor, Hackers Are There: The Need for Data Security Legislation and Cyber Insurance in Light of Increasing FTC Enforcement Actions.* New York: Brooklyn Journal of Corporate, Financial & Commercial Law.

Kaiser, S. A., & Mejia-Kaiser, M. (Vol. 64, Issue 2 (2015)). Cyber Security in Air and Space Law. *Zeitschrift fur Luft-und Weltraumrecht -German Journal of Air and Space Law,*, 396-412.

László, K. (2018). *Cyber Security Policy and Strategy in the European Union and Nato.* Sciendo, 2018: Revista Academiei Forţelor Terestre.