Secure Network Design

Wen Lun Hsu
Master's Student, Cybersecurity
New York Institute of Technology
Vancouver, Canada
whsu05@nyit.edu

Jay Ashokbhai Dangar
Master's Student, Cybersecurity
New York Institute of Technology
Vancouver, Canada
jdangar@nyit.edu

Hanu Deol
Master's Student, Cybersecurity
New York Institute of Technology
Vancouver, Canada
hdeol@nyit.edu

***Abstract*—This research paper gives an overview of the provided network infrastructure. It briefly discusses possible vulnerabilities and consequences when the security is compromised. We will also be discussing the possible remedies to counter particular attacks such as DDoS, Ransomware attacks, and Man in the middle (MITM). We will explain in great depth with some appropriate reasons as to why and when a particular solution is applied.**

Keywords — Man In The Middle Attack (MITM), Distributed denial-of-service (DDoS) Attack, Ransomware Attack, Online Reservation Systems, Threats and Vulnerabilities, Security Department

I. Introduction

The Van615 is a medium-sized hotel. It has an online reservation system where individuals can book their room remotely using the internet by accessing the Hotel website, and it also provides high-speed internet to its guests in the public area and the rooms refer to Figure 1 and 2. Recently the hotel had several security incidents which resulted in data breaching, data loss, and operations breakdown. These attacks resulted in the loss of customers' information, unavailability of services, and vulnerability in internal networks. These breaches and attacks are due to loose security plans and poorly defined security configuration, policies, and guidelines.

II. Threats and Vulnerabilities

In this section, we will be discussing the possible threats and vulnerabilities inside provided hotel network infrastructure. Security network architecture can be measured by analyzing how well it can achieve the Confidentiality, Availability and Integrity (CIA) schemes and the data transmitted between sender and receiver against possible attacks (Threats). We will firstly analyze the loopholes (vulnerabilities) inside the current network infrastructures. We briefly described possible sets of attacks and their countermeasures in Figures 4, 5 and 6.

III. Secure Architecture

A. Confidentiality, Integrity

- MITM attacks can be prevented or detected by two means: data integrity scheme and tamper detection. Authentication provides some degree of certainty that

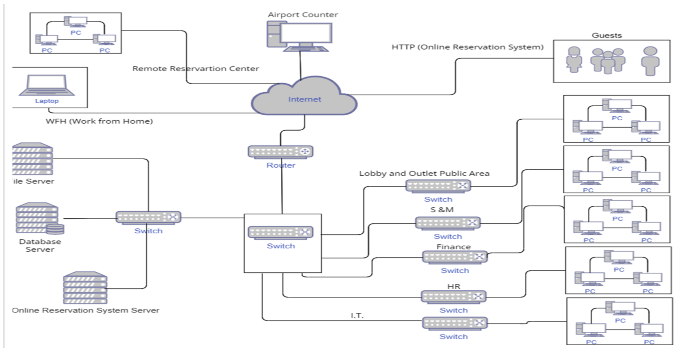


Fig. 1. Van615 Hotel Network Infrastructure

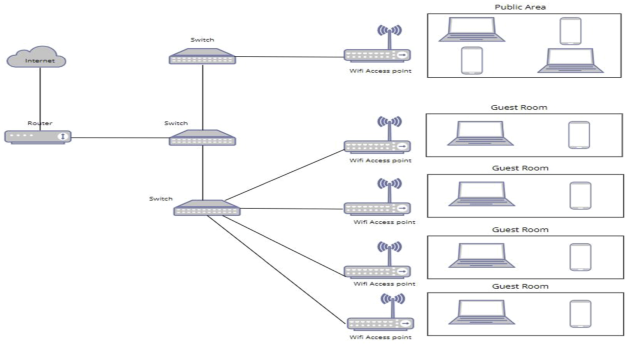


Fig. 2. Van615 Hotel Network Access Infrastructure

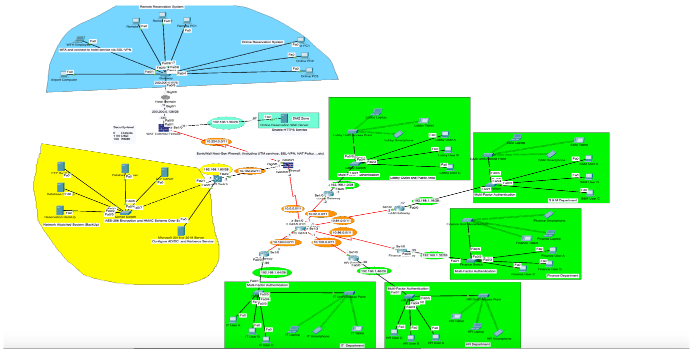
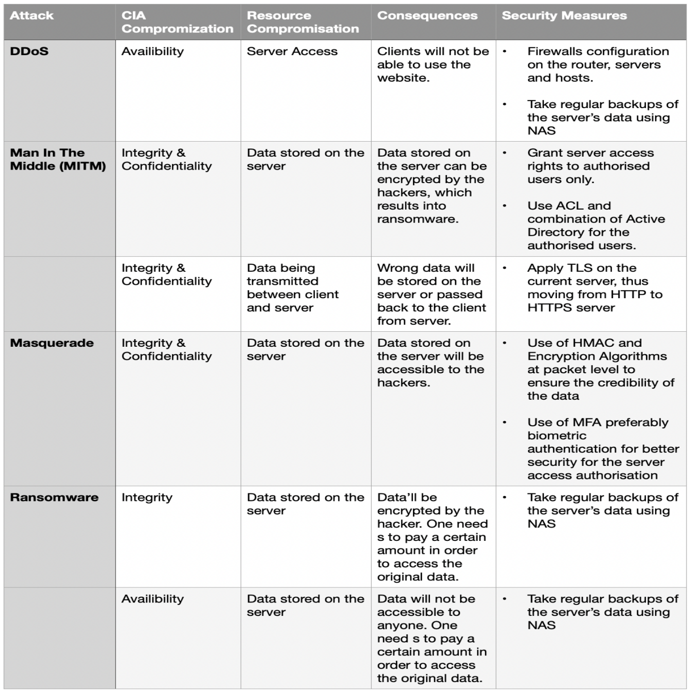


Fig. 3. Secure Network Topology



Attack	CIA Compromization	Resource Compromisation	Consequences	Security Measures
DDoS	Availibility	Server Access	Clients will not be able to use the website.	• Firewalls configuration on the router, servers and hosts. • Take regular backups of the server's data using NAS
Man In The Middle (MITM)	Integrity & Confidentiality	Data stored on the server	Data stored on the server can be encrypted by the hackers, which results into ransomware.	• Grant server access rights to authorised users only. • Use ACL and combination of Active Directory for the authorised users.
	Integrity & Confidentiality	Data being transmitted between client and server	Wrong data will be stored on the server or passed back to the client from server.	• Apply TLS on the current server, thus moving from HTTP to HTTPS server
Masquerade	Integrity & Confidentiality	Data stored on the server	Data stored on the server will be accessible to the hackers.	• Use of HMAC and Encryption Algorithms at packet level to ensure the credibility of the data • Use of MFA preferably biometric authentication for better security for the server access authorisation
Ransomware	Integrity	Data stored on the server	Data'll be encrypted by the hacker. One need s to pay a certain amount in order to access the original data.	• Take regular backups of the server's data using NAS
	Availibility	Data stored on the server	Data will not be accessible to anyone. One need s to pay a certain amount in order to access the original data.	• Take regular backups of the server's data using NAS

Fig. 4. Van615 Hotel Threats And Vulnerabilities

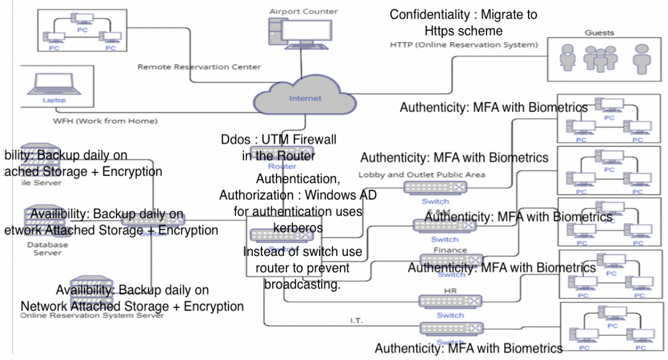

PC
PC
PC
Airport Counter
Confidentiality : Migrate to Https scheme
HTTP (Online Reservation System)
Guests
Remote Reservartion Center
Laptop
Internet
WFH (Work from Home)
Authenticity: MFA with Biometrics
Ddos : UTM Firewall in the Router
Router
bility: Backup daily on ached Storage + Encryption
ile Server
Authentication, Authorization : Windows AD for authentication uses kerberos
Authenticity: MFA with Biometrics
Lobby and Outlet Public Area
Switch
Availibility: Backup daily on etwork Attached Storage + Encryption
Database Server
Authenticity: MFA with Biometrics
Switch
Finance
Instead of switch use router to prevent broadcasting.
Authenticity: MFA with Biometrics
Switch
HR
Availibility: Backup daily on Network Attached Storage + Encryption
Online Reservation System Server
I.T.
Switch
Authenticity: MFA with Biometrics

Fig. 5. Secure Van615 Hotel Architecture

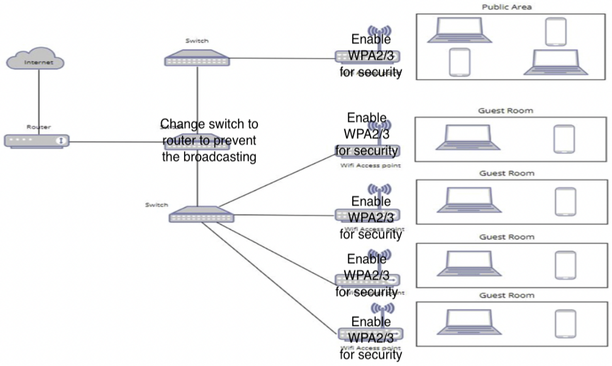

Public Area
Switch
Internet
Enable WPA2/3 for security
Router
Change switch to router to prevent the broadcasting
Enable WPA2/3 for security
Guest Room
Wifi Access point
Switch
Guest Room
Enable WPA2/3 for security
Guest Room
Enable WPA2/3 for security
Guest Room
Enable WPA2/3 for security
Wifi Access point

Fig. 6. Secure Van615 Hotel Architecture

a given message has come from a legitimate source. Tamper detection merely shows evidence that a message may have been altered.

– Data Integrity Scheme : Transport Layer Security, may harden Transmission Control Protocol against MITM attacks. In such structures, clients and servers exchange certificates which are issued and verified by a trusted third party called a certificate authority (CA).

– Temper Detection Solution : HMAC encrypts variable length plain text into fixed length cipher text, the generated code is added to the original message for msg authentication. Both the parties will share a secret key, which will be used for the encryption and decryption of the whole msg, which ensures the confidentiality part of the message.

- Hypertext Transfer Protocols Secure (HTTPS) - HTTPS is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase the security of data transfer.

  According to [3], data sent using HTTPS is secured via the Transport Layer Security protocol (TLS), which provides three key layers of protection:

  1) Encryption: Encrypting the exchanged data to keep it secure from eavesdroppers. That means that during the transmission of the data, no one can have the access to the original data.

  2) Data integrity: Data cannot be modified or corrupted during transfer, intentionally or otherwise, without being detected.

  3) Authentication: Proves that your users communicate with the intended website. It protects against man-in-the-middle attacks and builds user trust, which translates into other business benefits [5].

- Recommendations - Old protocol versions are vulnerable; It's recommended to use latest and newest versions of TLS libraries, related certificates and newest protocol versions. We also need to implement mechanism to validate the content after applying TLS, such that our content of HTTP and HTTPS needs to be same.

- Database encryption : Database encryption is a process to convert data in the database to "ciphertext" (unreadable text) using an algorithm. We need to use a key generated from the algorithm to decrypt the text. Recently cyber-attacks, data theft, or data breaches have been rampant; therefore, there is an increasing concern over private data.

1) AES: The Advanced Encryption Standard is a symmetric algorithm and is considered very secure. In fact, everyone from the U.S. government to software and hardware companies utilizes this algorithm. This method uses a block cipher rather than a bit-by-bit stream cipher. The block lengths are either 128, 192, or 256 bits. Users must share the key in order for others to access the data, which means they must also secure that key to prevent unauthorized access.

2) RSA: Rivest-Shamir-Adleman is an asymmetric algorithm that uses a public key for encryption and a unique private key for decryption. This method is typically used for sharing data over an insecure network, which can include database encryption. The key size is between 1024 and 2048 bits, which provides higher security but at a significantly slower pace than other methods.

B. *Accountability, Authentication, Authorization*

- Multi Factor Authentication: Multi-factor authentication (MFA) is a multi-layered security system that verifies the identity of users for login or other transactions. By leveraging multiple authentication layers, even if one of the layers is compromised, the user's account will remain secure.

  MFA generally refers to five types of authentication factors which are expressed as:

  - Knowledge: Something the user knows, like username, password, or a PIN.
  - Possession: Something the user has, like a safety token.
  - Heritage: Something the user is, which can be demonstrated with fingerprint, retina verification, or voice recognition.
  - Place: Based on the user's physical position.
  - Time: A time-based window of opportunity to authenticate like OTP.

  MFA includes adding biometric authentication and traditional authentication for the staff/employees accessing the central system. In this scenario, even if the hacker gets the access of the employee's credentials, they will find difficult to bypass the biometric authentication, which makes the system secure.

- Active Directory: Active Directory (AD) is a service which can enable on windows server and it uses Kerberos version 5 as authentication protocol in order to provide authentication between server and client. Kerberos protocol is built to protect authentication between server and client in an open network where other systems also connected. Kerberos system ensures authorised access to the resources.

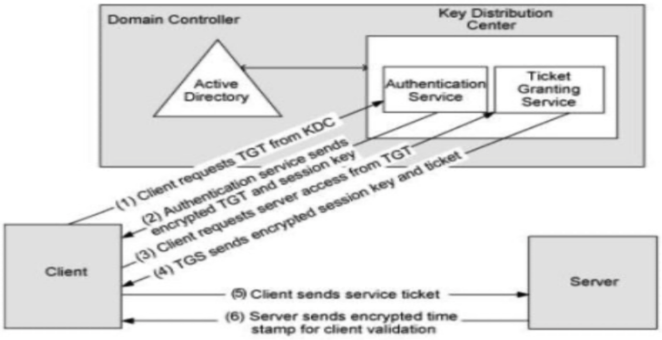

Domain Controller
Key Distribution Center
Active Directory
Authentication Service
Ticket Granting Service
(1) Client requests TGT from KDC
(2) Authentication service sends encrypted TGT and session key
(3) Client requests server access from TGT
(4) TGS sends encrypted session key and ticket
Client
Server
(5) Client sends service ticket
(6) Server sends encrypted time stamp for client validation

Fig. 7. Active Directory Kerberos System

- Wireless Security WPA2 and 3: When we install WiFi access point, router provides a few security options. If your router is unsecured, someone could access it, use it for illegal activities, like tracking your internet use [4] or even installing malware.

  - WPA2 - It has a stronger security and is easier to configure than the prior options(WPA). The main difference with WPA2 is that it uses the Advanced Encryption Standard (AES) instead of TKIP. AES is able to secure top-secret government information, so it's a good option for keeping a personal device or company WiFi safe.
  - The only notable vulnerability of WPA2 is that once someone has access to the network, they can attack other devices connected to the network. This is an issue if a company has an internal threat, such as an dismayed employee, who hacks into the other devices in the company's network.
  - WPA3 - As vulnerabilities are recognized, advancements are made. In 2018 [2], the WiFi Alliance introduced WPA3. This new version will have, "new features to simplify WiFi security, enable more robust authentication and deliver increased cryptographic strength for highly sensitive data markets." WPA3 is still being implemented, so WPA3-certified hardware is still not an available option for most people.

C. *Availability*

- Network Attached System (NAS Back-Up system) : DDoS Attacks are extremely difficult to prevent. By using NAS as a backup system, Organisation can prevent the possibility of loss or modification of the data. In order to setup the proper backup system, we need to follow certain guidelines :

1. Apply Encryption on saved data
2. Ensure unauthorized modifications of data.
3. Air gapping simply means storing the backup data in a different area that ia offline and physically separated from where it is being generated.

The 3-2-1 Rule

- 3 copies of your data
- 2 media types for your backups
- 1 backup stored in an offsite location

Coverage : Ensuring your backup solution covers your entire corporate data infrastructure is paramount to recovering every piece of critical data after a ransomware attack.

IV. Conclusion

Overall, we divided the project into two parts to achieve the goal, research and implementation.

1) We decide to add the various security schemes to the research part as to the research. TLS scheme, Wireless Security(WPA2/3), and database encryption algorithms can provide confidentiality. Additionally, HMAC and Multi-Factor Authentication can provide integrity and authenticity. Network Attached System(NAS) can provide availability, Active Directory Service with Keberos system can provide authenticity, authorization and accountability. Furthermore, Web Application Firewall is associated with DMZ, which can provide specific security schemes over the application layer.

2) As for the implementation section (Figure 3), configuring router routing and gateway can prevent the broadcast storm, ensuring the internal users can access the servers behind the internal firewall. More importantly, establishing the DMZ zone between the external firewall (web application firewall) and the internal firewall allows remote employees and public users to access the needed resources like the online reservation system. In addition, setting the Active Directory with the Kerberos system ahead of the critical servers can authenticate every internal user's requests in advance. Unfortunately, the Active Directory with Kerberos system can not implement via Cisco packet tracer because those are the services over the Windows Server in the real world. Last but not least, configuring the wireless security (WPA2-PSK)with access points in each one of the departments to secure the internal connection.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, ”On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] ”Fi Alliance® introduces Wi-Fi certified WPA3™ security,” Wi. [Online]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security. [Accessed: 09-Apr-2022].

[3] ”Transport layer security,” Wikipedia, 09-Apr-2022. [Online]. Available: https://en.wikipedia.org/wiki/Transport_Layer_Security. [Accessed: 09-Apr-2022].

[4] “How to track your life - panda security,” Panda Security Mediacenter, 04-May-2018. [Online]. Available: https://www.pandasecurity.com/en/mediacenter/tips/how-to-track-your-life/. [Accessed: 09-Apr-2022].

[5] “Man-in-the-middle attack,” Wikipedia, 25-Mar-2022. [Online]. Available: https://en.wikipedia.org/wiki/Man-in-the-middle_attack. [Accessed: 09-Apr-2022].

Appendix

Team Meeting 1

- Date: Tuesday, March 22, 2022
- Time: 1:00 p.m. - 14:00 p.m.
- Place: NYIT BTC Campus, 2955 Virtual Way
- Present: Jay Ashokbhai Dangar , Wen Lun Hsu, Hanu Deol

Agenda: Each member provide their ideas about these unsecure topology in terms of figure 1 and 2. Decision: Do some preparation and research related vulnerabilities Next steps:

- Prepare for next meeting: Tuesday, March 29, 2022
- Time: Time: 1:00 p.m. - 15:30 p.m.
- Place: NYIT BTC Campus, 2955 Virtual Way

Team Meeting 2

- Date: Tuesday, March 29, 2022
- Time: 1:00 p.m. - 15:30 p.m.
- Place: NYIT BTC Campus, 2955 Virtual Way
- Present: Jay Ashokbhai Dangar , Wen Lun Hsu, Hanu Deol

Agenda: Analyzing the vulnerabilities and brainstorming what are the approaches could secure the hotel network

Decision: Distributing the works and organizing the milestone to each one of us

Next steps:

- Prepare for next meeting: Tuesday, April 4th, 2022
- Time: Time: 1:00 p.m. - 16:30 p.m.
- Place: NYIT BTC Campus, 2955 Virtual Way

Team Meeting 3

- Date: Tuesday, March 29, 2022
- Time: 1:00 p.m. - 15:30 p.m.

- Place: NYIT BTC Campus, 2955 Virtual Way
- Present: Jay Ashokbhai Dangar , Wen Lun Hsu, Hanu Deol

Agenda: Integrating the distributed works and Wen Lun Hsu demo the implementation part to group members
Decision: Polishing the research report

Responsibility

Member: Wen Lun Hsu

- Based on Fig 1 ,2 and the security schemes, implement and create a new topology (Fig 3) via packet tracer
- Configure the routing table in order to prevent broadcast storm
- Implement DMZ zone and Web Application Firewall

Member: Jay Ashokbhai Dangar:

- Research about Network Attached System (NAS Back-Up system)
- Research about HMAC code prevent MITM
- Research about MFA scheme to protect intrenet
- Research about Windows Active Directory and Kerberos System

Member: Hanu Deol:

- Research about HTTPS scheme and how could it protect web server
- Research about Wireless WPA2 or 3 Security
- Research about Database encryption