Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 1

Kin Wong

Initial Post

19 days ago

6 replies

Last 7 days ago

The major threats and vulnerabilities:

Brute force attack: A brute force attack means a hacker keep guessing the login passwords, encryption keys, in order to get any privilege which can control the network and system (Kaspersky, 2021).

The brute force attack has created the threat of availability indirectly (The network connection has been hijacked and become unavailable) and confidentiality (The network packets would be captured and exposed).

DDOS: After the Wi-Fi has been cracked, the hackers deploy DDOS, create massive network traffic into the Wi-Fi network, overwhelming the iStan system and Wi-Fi Network and disrupt whole connection (Cloudflare, 2021), making iStan become failed.

DDOS attack will cause the threat of availability and integrity (Data loss due to the disruption).

Solutions:

For Brute force attack: Deploy MFA: Besides a usual password, MFA requires additional form of identification, from send a one-time passcode to your cell phone to providing a fingerprint scan (Microsoft, 2021). MFA will make brute force attack become useless.

For DDOS: A stateful firewall in front of the Wi-Fi network, which can inspect layers 3 and 4 OSI layers, able to keep track of every network connection and recognise any potential risk and block it, including the DDOS attack. (Fortinet, 2021)

References:

Kaspersky (2021) Brute Force Attack: Definition and Examples, Available at: https://www.kaspersky.com/resource-center/definitions/brute-force-attack (Accessed: 5th May 2021).

Cloudflare (2021) What is a DDoS Attack?, Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Accessed: 5th May 2021).

Microsoft (2020) How it works: Azure AD Multi-Factor Authentication, Available at: https://docs.microsoft.com/en-GB/azure/active-directory/authentication/concept-mfa-howitworks (Accessed: 5th May 2021).

Fortinet (2021) Stateful Firewall, Available at: https://www.fortinet.com/resources/cyberglossary/stateful-firewall (Accessed: 5th May 2021).

Reply

6 replies

1 Post by **Laura Rivella**

15 days ago

Peer response

Hi Kin,

While I do agree with your proposed mitigation for brute force attacks, I would still like to bring to the table the issue of the usability of MFA tools, which still remains one of the main challenges hindering user adoption of it. (Das, Dingman & Camp, 2018).

While it is certain that MFA dramatically improves security, the balance between security and usability remains the main concern in its adoption. (Braz & Robert, 2006)

As with most people-centered issues in security, rate of adoption and use of MFA could be improved by providing background knowledge and risk trade-offs of non-adoption before deploying MFA. Employers and sysadmins should also consider providing detailed step-by-step instructions for setting up MFA to improve chances of user buy-in.

References

Braz, C. & Robert, J. M. (2006) Security and Usability: the Case of the User Authentication Methods. IHM 6: 199–203.

Das, S., Dingman, A. & Camp, L. J. (2018) 'Why Johnny doesn't Use Two Factor a Twophase Usability Study of the Fido u2f Security Key', in: Kadianakis, G, Roberts, C.V., Roberts L. & Winter, P. Financial Cryptography and Data Security. Springer Berlin Heidelberg.

Reply

2 Reply to **Laura Rivella** from **Doug Millward** ↑

14 days ago

Feedback

I left you a comment about 2FA/ MFA before I read this :)

As always some very good points and a valid argument about usability vs security.

Reply

3 Reply to **Laura Rivella** from **Shiraj Ali** ↑

12 days ago

Re: Peer response

Glisson et al. (2015) discussed the threats and vulnerabilities in the iStan system and Wi-Fi Network, and one would classify iStan as an IoT device. However, I am not sure how MFA will help, as most IoT device do not use MFA. I think it will be tricky to use MFA on IoT devices, and it may be possible, but it will be an administrative nightmare.

Reply

4 Post by **David Luvaha**

11 days ago

Peer Response

Additionally, according to NHS Digital (2020) weaknesses found in medical solutions will remain unpatched within supplier's evaluation period and are exploited by unskilled hackers. To diminish the risk, firstly, decrease the probability of breaches by stopping the devices from accessing untrusted content. Secondly, diminish the impact of breaches by averting access to sensitive data or services from vulnerable medical hardware. An effective mitigation plan must have a blend of these two tactics.

References

NHS Digital (2020) Step 2. Create a Mitigation Plan
Available from:
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices
[Accessed 13 May 2021].

Reply

5 Post by **Jan Küfner**

8 days ago

peer response

The medical mannequin described by Glisson et. al. (2008) could easily be attacked since the network was not well secured. A firewall as mentioned in the initial post by Kin Wong is a very good defense mechanism, nonetheless there are three more pillars to a secure network than traffic filtering according to Ross (2008):

* Securing the network by continuous SW updates and HW replacements

* Intrusion Detection

* Encryption of valuable information assets (e.g., patient data), if any

By following the first recommendation, all attacks described in the article by Glisson et. al. (2008) would have been mitigated, since the medical mannequin was using an outdated Wi-Fi Protocol (WPA).

References

Glisson, W., Andel, T., Mc Donald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015) 'Compromising a Medical Mannequin', 21st Americas Conference on Information Systems. Fajardo, Puerto Rico, 13-15 August.

Ross, A. (2008) Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition. Indianapolis: Wiley Publishing Inc.

Reply

Maximum rating: -

6 New Post by **Kin Wong**

7 days ago

Summary Post

About the MFA usability, Microsoft (2021) has proposed different ways and medias for the MFA, including SMS, Voice phone calls, authenticator app, software and hardware tokens, security key and her own Windows Hello technology. I can choose which authentication is easy and suitable for myself and other staffs.

With different choices of authentication method, MFA will become more flexible and easier to deploy. I also can choose which authentication method depends on the cost. For example, I can install authentication app and SMS for one time password as my authentication method, instead of hardware token and FIDO2 security key, which need to be purchased with extra cost.

Although the MFA can eliminate the brute force attack, the firewall or any network security appliance, including the IDS and WSA, which can prevent most of the potential security threats. But the biggest risk which will cause any cyber security vulnerability is the human factor (Cisomag, 2020).

Human errors will cause any cyber security measure to be failed. One example is social engineering. Attacker will research the target's status, such as what is his/her job responsibility and what authority/company he/she always contact. Attackers able to pretend the relevant party, develop and gain the trust with the target, and receive any sensitive information, which is delivered by the target actively. In this case, any cyber security measure will become useless (Springer Nature, 2018).

In order to mitigate the human error, Ekran (2021) suggests different solutions. Firstly, security policy should always be updated, from the handling of critical data, which software can use, etc.

Education to employee is also important. They need to know how to recognise and aware any potential threats, line manager should explain what the dangerous and expensive consequences are if they have created any mistake.

Least privilege principle should be deployed to minimise the security threat, monitoring the employees' network activity and their network traffic are also essential.

References:

Microsoft (2021) *Secure access to resources with multifactor authentication,* Available at: https://www.microsoft.com/en-gb/security/business/identity-access-management/mfa-multi-factor-authentication (Accessed: 11 May 2021).

CISOMAG (2020) *What is the "Cyberchology of Human Error" in Cybersecurity?,* Available at: https://cisomag.eccouncil.org/human-error-in-cybersecurity/#:~:text=Human%20error%20was%20the%20biggest%20cybersecurity%20challenge%20for,their%20ability%20to%20manage%20stress%20during%20the%20crisis. (Accessed: 17th May 2021).

Ibrahim G, Jibran S, Mohammad H, Hanan F, Vaclav P, Sardar J, Sohail J, Thar B (2018) 'Security Threats to Critical Infrastructure: The Human Factor', *The Journal of Supercomputing,* 74(2)(10.1007/s11227-018-2337-2), pp. 4987-4991 [Online]. Available at: https://www.researchgate.net/publication/323907193_Security_Threats_to_Critical_Infrastructure_The_Human_Factor (Accessed: 17th May 2021).

EKRAN (2021) *How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes,* Available at: https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes (Accessed: 17th May 2021).

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post

NEWER DISCUSSION

Initial Post