Network and Information Security Management May 2021 A

Home / / My courses/ / NISM_PCOM7E May 2021 A / / Unit 1 / / Collaborative Learning Discussion 1 /

/ Initial Post /

« Collaborative Learning Discussion 1

Jan Küfner

Initial Post

13 days ago

5 replies

Last 20 hours ago

Adobe Flash Player and the OS environment (Windows or OS X) known for easy ways to exploit a device, if not patched, were touched as potential vulnerabilities of a medical mannequin discussed by Glisson et al. (2015). The article however focused on the wireless network communication between the mannequin and the control computer.

As stated by Glisson et al. (2015) Denial of Service (DoS) attack was one of two major threats that such a device can face. The DoS attack therefore was further investigated by Glisson et al. (2015).

The second major threat, that was identified by Glisson et al. (2015) was a brute force attack against the wireless network.

The following proposals for mitigation do have their limitations, since not all information of the usage of a medical mannequin are known. It is for example unknown, if the PC is distributed with the mannequin. It is also unknown, if one PC typically controls several mannequins or just one.

According to Ross (2008) any network should be secured via continuous and timely updates, filtering of traffic, intrusion detection and encryption. Since the mannequin does not have valuable credit card or patient information encryption is not necessary to apply. Those fundamentals of Ross (2008) can be applied for the example of the mannequin as stated below.

My proposal for mitigation against a brute force attack of the network in this situation are as follows:

1. Use state of the art wireless protocols (WPA-2, Bluetooth) instead of outdated and unsecure protocols (WPA)

2. Deactivate vulnerable features (WPS) of the network

3. Use wired connection only (e.g., cross-link cable), if feasible

4. Segregate the network from larger networks (apply traffic filtering)

5. Monitor the network for intrusion

6. Set up a VPN or SSH environment for the mannequins and their control computer

7. Add authentication and encryption in the application layer of the system software

My proposal for mitigation against a DoS attack is in this situation are as follows:

1. Secure network (see above items 1 - 5)

2. Limit unauthenticated traffic at device level / Drop communication packages at the devices to be able to handle authenticated traffic.

In conclusion it can be stated, that for this example there are easy ways to mitigate the threats discussed by Glisson et al. (2015)

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: 👍 (1)

5 replies

1 Post by **Kin Wong**

13 days ago

Peer response

I agree wired network should be used instead of wireless. The man-in-the-middle attack to the Wi-Fi network will be eliminated: the network is only communicated with physical cable connections; while the Wi-Fi signal is maintained by broadcasting, both inside and outside the building. Outsiders can capture the signals easily. (Dale, 2018)

Besides firewalls and IDS, anti-malware and anti-virus appliance and software are also essential, to eliminate the security threat and data loss due to the malware. Every device should have anti-virus software installed; OS based firewall should be deployed and block all unnecessary ports. The MacOS X has built-in firewall, which can specify which app and service can pass through the firewall; while stealth mode can protect the MacOS from being discovered by hackers and malware (Apple, 2021).

Despite of a wired network, VPN and SSH add one more protection to the data: IPSec is one of the most secured VPN technologies, which is a group of protocols being used together and setup encrypted connections (Cloudflare, 2021); while SSH is mainly used on secure remote desktop connections. Including strong cryptography and authentication, to prevent any spoofing; with agent forwarding, your authentication keys won't store in any other machine in the network; SFTP can transfer files with strong encryption (OpenSSH, 2021).

References:

Dale, S (2018) *Wired vs Wireless Networking,* Available at: *https://aberdeencybersecurity.co.uk/wired-vs-wireless-networking/* (Accessed: 11 May 2021).

Apple (2021) *Block connections to your Mac with a firewall,* Available at: *https://support.apple.com/en-gb/guide/mac-help/mh34041/mac#:~:text=%20Set%20firewall%20access%20for%20services%20and%20apps,to%20add.%20After%20an%20app%20is...%20More%20* (Accessed: 11 May 2021).

Cloudflare (2021) *What is IPsec? | How IPsec VPNs work,* Available at: *https://www.cloudflare.com/learning/network-layer/what-is-ipsec/* (Accessed: 11 May 2021).

OpenSSH (2021) *OpenSSH Features,* Available at: *http://www.openssh.com/features.html* (Accessed: 11 May 2021).

Reply

2 Post by **Doug Millward**

13 days ago

Feedback

Good recommendations and well thought out responses from both of you - good use of references as well.

Reply

3 Post by **David Luvaha**

11 days ago

Peer Response

Similarly, according to the NHS Digital (2020) the solutions such as antivirus, host-based and network-based intrusion detection systems can be deployed because they give some benefits in detecting malicious code. NHS Digital (2020) observes that their efficiency may be diminished due to the product not being updated during the supplier's assessment period. NHS Digital (2020) adds that Intrusion detection products situated on the biomedical devices segregated network may provide an early warning of malicious codes because they may be serviced and maintained and updated immediately new patches are released. However precaution need to be taken to confirm that implementing a path for updates to these intrusion detection devices does not bypass the network segregation controls needed for the biomedical devices on that same network.

References

NHS Digital (2020) Anti-malware and intrusion detection products
Available from:
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices
[Accessed 13 May 2021].

Reply

4 Post by **Charlotte Wilson**

10 days ago

Peer Response

Jan,

I agree with many of your proposed solutions to the threats identified within the paper. In particular the monitoring of the network for intrusion. I believe that monitoring is one of the more difficult things to get right in terms of security controls, but something that is necessary in mitigating security threats. One issue that must be overcome to make monitoring efficient, would be limiting the amount of false positives that exist within. By removing false positives, it allows for security professionals to mitigate real threats quicker and more efficiently. That being said, it is important to be 100% confident that a false positive is in fact a false positive. If not, real vulnerabilities could be left undetected and worse, ignored (White Hat Security, N/A).

One other mitigation that I would also suggest would be education / training of users of the device itself. Unfortunately, data breaches / cyber incidents can take minutes to compromise successfully; however, can take months or more to discover (Blosfield, E., 2019). Although a mitigation to be put in place once the above has been completed, I would argue this is necessary to ensure the security of the devices in the long term. Unfortunately, many end-users may not know what to look for or what could be deemed suspicious behaviour, so educating them expands the oversight security professionals have.

- White Hat Security (N/A) False Positive. Available from: https://www.whitehatsec.com/glossary/content/false-positive [Accessed 14 May 2021]
- Blosfield, E. (2019) Data Breaches That Take Minutes to Occur, Often Require Months to Discover. Available from: https://www.insurancejournal.com/news/national/2019/07/03/531283.htm [Accessed 14 May 2021]

Reply

5 Post by **Jan Küfner**

20 hours ago

Summary Post

The medical mannequin, typically used in hospitals to train doctors, described in the article by Glisson et al. (2015) started a valuable discussion with many very good contributions from my peers on how to secure a network, since the mannequin did not offer security capabilities itself such as e.g. application layer security.

The network in the article was utilizing an outdated protocol (WPA instead of WPA-2). Updates of hard- and software can easily prevent those vulnerabilities and therefore should be conducted on a timely basis. Ross (2008)

In general it can be stated, that having a firewall at the edge of the network and firewalls running on the individual clients are a very valuable addition to your layered defense. Network segregation by filtering traffic in e.g. switches is also a recommended technique to secure high risk areas of your network. Ross (2008)

Another valuable mitigation is host- or network-based monitoring for intrusion. Host based intrusion detection or prevention is done by e.g. antimalware and antivirus programs, which also should be installed, where possible. Ross (2008), NHS Digital (2020)

To secure unencrypted traffic in transit a VPN tunnel can be created. This technique is very effective, it will however consume resources such as money and staff time for implementation and maintenance. Ross (2008)

One of the weakest link might be the operator, that can start a ransomware attack by being a victim of a phishing attack or by plugging in a compromised device into the network. To mitigate this risk good and regular education is recommended. Wilson (2021)

In conclusion it can be stated, that a hardened network is a very valuable layer in your defense in depth approach. In scenarios, where the devices integrated do not offer up to date security capabilities a hardened hospital network is in some instances the key mitigation to an attack, which can lead to patient harm, loss of private health data, regulatory fines and reputational damage.

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.

NHS Digital (2020) Anti-malware and intrusion detection products. Available from: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices [Accessed 24.05.2021].

Wilson, C. (2021) Discussion Forum post by Jan Küfner, 14.05.2021

Reply

Maximum rating: -

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