Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 1

Czeska Stanley

Initial post

7 days ago

2 replies


Last 1 day ago

Upon reading the paper provided, I was surprised to read that this is a thing as I was not aware that this was even at all possible, although in hindsight, I suppose anything with technology is crackable.

Throughout the paper some of the main security concerns that I read included, but were not limited to the following:

- Knock on effect of attacks from devices to training facilities
- Inaccurate feedback from medical devices
- Tracking the patient
- Revealing PII
- Cloning the patient details and possibly the patient (identity fraud)
- Altering patient medication via devices that administer drugs

On the basis of furthering knowledge and being able to mitigate future potential attacks, Halperin et al have tried and accomplished the successful hacking of a pacemaker to ascertain what PII (personal identifiable information) they were able to harvest.
The result of this test was that they were able to obtain the patient records and also change the way the pacemaker behaves.

Some ways of mitigating these vulnerabilities mostly consist of having a strong password consisting of numbers, letters and symbols and not using the generic PIN that comes with it. By employing this method of defence, this prevents brute force attacks, dictionary attacks and rainbow table attacks to an extent.

References

Halperin, D. et al. 2008a. "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in: Proceedings of the 2008 IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 129-142

Reply

2 replies

1  Post by **Jan Küfner**

3 days ago

Peer response

Pacemakers and implantable cardioverter-defibrillator come with many challenges. Hardware typically cannot be upgraded. Battery consumption / cycle time of integrated circuits (ICs) and main control units (MCUs) need to be at a minimum to extend battery longevity to ultimately reduce or delay any replacement surgery.

On the other hand, those implants do have high value assets for cyber criminals. Performing an attack for example, that shuts off this life sustaining device are likely to obtain high value ransoms. Attacks on individuals are however not yet reported, but an unethical disclosure of such a vulnerability was done to short the stock market. (Finkle & Burns 2016).

To successful mitigate attacks in those devices an extremely high level of cyber security must be in place. It is therefore a very good idea to double efforts. Wireless links for example can be authenticated and encrypted twice. This will have the benefit, if a vulnerability severe for medical devices such as e.g., Sweyntooth (NIST 2019) is discovered in one of the protocols the device can still not easily be compromised, since there is another layer of defense that need to be broken by the attacker. Zero-day attacks still cannot be stopped, the device is at that time however not yet fully compromised and more resources need to be spend by the attacker, which is likely to prevent many attacks.

The challenge however is to create chips, that economically perform those encryption operations.

References:

Finkle, J. Burns, D. (2016) St. Jude stock shorted on heart device hacking fears; shares drop. Available from: https://www.reuters.com/article/us-stjude-cyber-idUSKCN1101YV Accessed on 2021-05-21

NIST (2019) CVE-2019-16336. Available from https://nvd.nist.gov/vuln/detail/CVE-2019-16336 Accessed on 2021-05-21

Reply

Maximum rating: -

2  Post by **Dinko Isic**

1 day ago

Peer Response

According to the recent Forescout Research Labs (2020) at least 75 percent of healthcare entities are impacted by a these three TCP/IP vulnerabilities: NUMBER:JACK - allows the attacker to bypass authentication, hijack or spoof TCP connections, launch DoS conditions, or inject malicious data; NAME:WRECK - impacts the DNS that enables a requesting device to resolve desired domain names to specific IP addresses and AMNESIA:33 - an exploit that could lead to remote code execution, allowing an attacker to take full control of a device (Davis, 2021).

Although these vulnerabilities impact the devices across various sectors, the Forescout Research Labs (2020) discovered that healthcare is at a higher risk than other industries, primarily because of the range of devices used by healthcare organizations and the high diversity of vulnerable vendors. Hospitals and healthcare entities also have a host of devices that are always on or in use, which increases the risk of exposure.
The most vulnerable medical devices are infusion pumps, patient monitors, and point-of-care diagnostic systems.

New research from Cynerio (2021) shows that healthcare must adopt a zero-trust architecture that will significantly reduce ransomware, outdated firmware, and unsecured services by configuring policies that block unnecessary communications with healthcare devices.

It is necessary for healthcare organizations to implement measures to support proper network segmentation in order to protect vulnerable devices that cannot be patched. For instance, only traffic from or two allowed devices should be permitted.

It is also crucial to implement a response plan that can be launched as soon as an intrusion is suspected or confirmed. Such a plan should include tools and mechanisms to detect the intrusion and affected assets, recording activity logs, and respond to intrusion by isolating affected devices or blocking connections from/to the attacker (Davis, 2021).

Resources:

Cyberio. (2021) Healthcare organizations must choose zero-trust architecture. Available from: https://industrialcyber.co/vendor/cynerio/ [Accessed 23 May 2021].

Davis, J. (2021) Report: Healthcare IoT, Devices Most Impacted by TCP/IP Vulnerabilities. Available from: https://healthitsecurity.com/news/report-healthcare-iot-devices-most-impacted-by-tcp-ip-vulnerabilities [Accessed 23 May 2021].

Forescout Research Labs. (2020) *Connected Medical Device Security: A Deep Dive into Healthcare Networks.* Available from: https://www.forescout.com/company/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks [Accessed 23 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