harborlabs
CYBER . SCIENCE

MEDICAL DEVICE SECURITY

Best Practices for Ensuring Cybersecure and Cybersafe Medical Device Design

The internet of medical devices (IoMD) within a health care facility comprises a broad array of technologies, ranging from simple physiological instruments such as thermometers and pulse monitors, to sophisticated imagery and therapeutic systems with extensive computing resources and high-bandwidth networking. The bedside systems found in patient rooms, including pumps, sensors, and the nurses' cart-on-wheels are not only networked, but are often directly connected to patient databases and billing centers. Unlike other computing platforms on the network, networked medical devices are designed primarily for their medical function, with less consideration given to the authentication technologies and cyberdefenses typical of other IT. Moreover, the open nature of most medical facilities makes it possible to conduct on premises attacks, either through a close proximity wireless exploit, or through a direct network connection. The especially valuable and vulnerable set of targets in the IoMD and has led to the newest form of exploitation in the cybersecurity vocabulary: medjack: a medical device hijack.

But far more than just a backdoor into the financial targets of the network, medical devices are a critical and highly exposed set of targets themselves. For a cybervandal, criminal or terrorist, gaining root access to a medical device can be the functional equivalent of gaining root access to the patient, making medical devices an extremely attractive target for attackers specializing in ransomware exploits. The ability to disrupt, stop, or purposefully control critical systems, such as a drug infusion pump or respiratory and cardiac equipment, gives the attacker direct control over patient safety and health. A malicious actor can pivot from a compromised IT asset on the medical network to a medical device and either exploit the device directly or alter its therapy with the intent of doing harm to the very patient the device is treating.

Medical Device Vulnerability

As well defensed as today's medical networks may be, the fact that they are nonetheless routinely exploited by a determined and ever-evolving cyberattacker community is well publicized. And once inside the hospital enterprise, the hacker's kill chain begins with a reconnaissance of the network and identification of the most vulnerable pivot points. Medical devices, almost by design, present a wealth of readily available targets. Openly visible, accessible, and with minimal cyberdefenses, they serve as a ready foothold from which to conduct exploits and exfiltration.

These vulnerabilities make it possible to conduct medjacks on premises through a wireless attack, directly via an unmonitored wired network port in the facility, or indirectly through a compromised network asset, such as a workstation or offsite system. The convenience and increasing need for wireless portability within the medical facility compounds the risks even further, as medical devices are moved between rooms, floors and wards, and their wireless signals are broadcast indiscriminately beyond a controllable radius.

The Defensive Challenge

While the primary identity of a medical device is its therapeutic function, it is nonetheless still an IT endpoint. Built on the same computing platforms and common operating systems as many other IT systems, medical devices are likewise subject to the same set of cyber vulnerabilities and attack methods.

whitepaper

But unlike other IT systems, medical devices typically lack the auxiliary resources necessary to support built-in or add-on 3rd-party endpoint security solutions such as anti-virus, eventing, firewalling and host-intrusion detection systems. Complicating this challenge even more is the fact that under no circumstances can a security solution function in a way that could inadvertently block or impede valid use of the medical device.

There are devices in use in clinical networks today with known vulnerabilities. Many of these devices contain globally shared secrets that allow an attacker to reverse engineer only one device in order to gain privileged access to any device of the same model. Some devices allow unauthenticated telnet access to be enabled either as a debugging feature, a management feature, or through exploit. Many lack any exploit mitigation functionality, and some are vulnerable to simple buffer overflows. Drug libraries and prescription information are often sent to devices without any authentication. As industry practices and cyber awareness improve, some of these oversights are beginning to be addressed, but many devices currently in operation, and legacy systems in particular, are still subject to these exploit categories.

Even newly released devices frequently use incorrectly designed or improperly implemented cryptographic protocols--protocols that allow attackers to compromise data privacy and integrity. The training and expertise necessary to ensure a sound cryptosystem is often too specialized for the software development team assigned to a medical device, requiring the assistance of 3rd-party cryptographic expertise. But the need for this special expertise may not always be apparent to a manufacturer, as even subtle flaws in the cryptographic implementation can have deleterious results. For example, the order in which data is encrypted and authenticated may impact the entire system. A broken cryptographic protocol is a particularly difficult issue to fix. All devices speaking the protocol, as well as all control and management servers, must be upgraded in parallel in order to correctly address the underlying issue. This could comprise thousands of devices in a single clinical environment. Unfortunately, the manufacturer often does not know that the protocol design was insecure until after the vulnerability is discovered and made public.

The diligence of the medical device manufacturer community and their increasing awareness of the need for device security is an encouraging sign in an industry faced with a daunting set of cyber challenges. Unlike other IT systems which are designed to provide a rapid response to security vulnerabilities as they are exposed, and routinely provide proactive maintenance and security patches in response to potential threats, medical device patches are typically more reactive. As has been demonstrated by some recent, well-publicized device exploits, the remedies to known vulnerabilities can require long research and development cycles. These security lags are impractical for keeping pace with the cybercriminal community, resulting in either the device being taken offline, or continuing operation with a known vulnerability.

Medical Device Secure Design

Given the inherent limitations of securing medical devices, device manufacturers are compelled to give greater scrutiny to the firmware, software, communication protocols, topologies and operations of their devices prior to being released into the market. Rather than rely on traditional 3rd-party perimeter cyberdefenses, manufacturers are investing in secure design processes and secure software architectures to ensure the cybersafety of their devices as part of their go-to-market strategies. By focusing on the security of the device itself, medical device manufacturers are taking ownership of their own security obligations

and giving their customers confidence in their product lines.

Manufacturers can significantly improve their security outcomes by adhering to a common set of best practice design and coding principles. By integrating security and privacy into early-stage design and test phases, rather than treating these concepts as after-market remedies, medical products can get to market more quickly and with greater cybersecurity and resilience.

Cybersecurity Best Practices

Device manufacturers are increasingly employing cryptography professionals and secure coders as part of their development teams to design cryptographic controls and system security into their protocols before implementation. A trained cryptography expert is essential in the device design phase, as cryptography has many highly varied and complex components. Key management and distribution, revocation, and protocol design and implementation all have many options that, when not properly designed, can lead to completely ineffective cryptography. An experienced cryptographer can help a medical device manufacturer understand how to apply cryptography correctly, and in a way that best addresses the needs of all stakeholders. Getting crypto right during the device design phase is of paramount importance. It is often impossible to retrofit cryptography into a device as an aftermarket solution, and once exploited, weak cryptography can be extremely expensive to fix.

Companies are hiring security engineers to design and build security controls into their management platforms and into their devices. Security engineers work in coordination with the medical device manufacturer, collect requirements, review existing product development documentation and resources, and design a specific plan to address the security concerns of the device manufacturer across all possible deployment environments. Security engineers can help a medical device manufacturer to consider security at all layers of the software and hardware stack, including network interfaces and associated communications protocols, and can help determine where to apply the most resources given the challenges that are unique to the target device. These engagements lead to improved outcomes in device security, as everything from access control, to wireless protocols, to authentication, to vulnerability assessment and patch management can be considered and addressed on a device-specific basis.

Firmware and Software Security Audits

Security is a process, and new vulnerabilities and exploitation techniques are developed on an ongoing basis, leading to the compromise of devices once thought to be secure. As part of validating device security prior to market release, and as part of maintaining a sound security posture, companies are hiring code auditors to perform static and dynamic vulnerability analyses on their software to manually validate code security prior to being released. These companies will often also commission penetration tests. When conducted in an environment and topology that simulates the clinical network, these pen tests are an ideal method of exposing vulnerabilities in a real-world operational setting. Each of these steps can dramatically decrease the likelihood that a medical device will be compromised once deployed in a clinical environment.

Another security best practice that is commonly followed prior to releasing a medical product is code

auditing. An experienced code auditor will audit the source code using a combination of static and dynamic analysis techniques, with the understanding that these techniques and the related auditing tools can commonly lead to both false positives and false negatives. Tools are no substitute for an experienced code auditor. A good source code auditor can cut the false positive rate from these automated tools down to near zero while simultaneously looking for flaws that automated tools frequently miss, such as architectural vulnerabilities and race conditions.

Similarly, an experienced penetration tester can catch vulnerabilities that otherwise go undetected in the design phase. Firmware is typically composed of manufacturer-built applications running on third party platform code. Errors in platform configuration can lead to a complete compromise of the entire system. No matter how diligently source code has been analyzed, it will never be completely free of bugs or security defects. Penetration testers can check for unknown defects in manufacturer-produced applications using advanced runtime analysis techniques, such as fuzzing and associated analytic instrumentation. And most importantly, the pen tester can check the platform for security issues arising from misconfiguration, and software vulnerabilities in the platform components.

Medical device security expertise is a unique skill, and experienced experts in the field can be difficult to find. Their unique perspective on medical security and practical usability, and the tensions between the two, is a critical skill in the secure design of medical devices. A security generalist might be able to offer a broad array of methods to lock down a medical system in the absence of constraints. But, the experienced medical security professional also considers how to handle the more nuanced situations that healthcare presents, such as emergency security bypasses, remote access, cloud connectivity and storage, and the challenges of in-home health systems. A comprehensive, multi-tiered approach to secure medical device design that includes cryptosystem expertise, secure software design and coding principles, code auditing, penetration testing, and operational practicality, are the crucial components of ensuring the cybersecurity and cyber resilience of networked clinical devices.

About Harbor Labs

Harbor Labs is a leading provider of cyber science consulting services, specializing in cryptography, network security audits, software vulnerability assessments, and secure programming. Our elite staff of cyberscientists comprises many of the industry's foremost experts in their respective cyber disciplines and are among the first to be contacted when a high-profile, national-level cyber event occurs.

info@harborlabs.com
1-833-CYBR SCI
106 Old Court Rd,
Suite 305, Pikesville,
MD 21208

whitepaper