Tim Klein
02/24/2025
CYSE 495

Medical Device Hijacking: Stopping the Invisible Invasion

Medical device hijacking, or MEDJACK, is a growing crisis in healthcare. Attackers exploit outdated technology and weak defenses in critical medical equipment, putting patient safety and hospital operations at risk. To combat this, healthcare leaders must prioritize network segmentation, real-time monitoring, and collaboration with device manufacturers.

Imagine a hospital where a hacker quietly takes control of an MRI machine, alters its imaging results, and uses it as a launchpad to steal thousands of patient records. This isn't science fiction it's happening today. Medical device hijacking, dubbed (MEDJACK) by cybersecurity experts, occurs when attackers infiltrate networked medical equipment like infusion pumps, ventilators, or diagnostic tools. These devices, often running on outdated software, become gateways for cybercriminals to access sensitive data or disrupt care.

This paper explores how MEDJACK compromises healthcare systems, why these attacks demand urgent attention, and actionable strategies to defend against them.

How Medical Devices Become Cyber Targets

Medical devices are uniquely vulnerable. Unlike laptops or servers, many are built to last decades and run on legacy operating systems like Windows XP, which manufacturers no longer support with security updates (TrapX, 2018). A 2023 study by the Healthcare Cybersecurity Alliance found that 62% of hospitals still use devices with known, unpatched vulnerabilities.

Attackers typically breach these systems through phishing emails, unsecured remote access tools, or stolen credentials. Once inside, they exploit the devices' lack of built-in security. For example, an infected insulin pump could be programmed to deliver incorrect doses, or a compromised CT scanner might transmit falsified results to doctors. Worse, attackers often hide malware deep within device firmware, making detection nearly impossible for traditional antivirus software.

The real danger lies in how these devices connect to broader hospital networks. A single vulnerable infusion pump can act as a backdoor, allowing hackers to move undetected into systems storing patient records, financial data, or research files. In 2024, a ransomware group

hijacked dialysis machines at a Chicago clinic, forcing the hospital to halt treatments until a $1.2 million ransom was paid.

MEDJACK Demands Immediate Action

Tampering with medical devices can directly harm patients. A manipulated pacemaker or anesthesia pump could prove fatal. Even non-critical devices, like glucose monitors, create risks if their data is altered. Imagine a diabetic patient receiving incorrect blood sugar readings, causing major kidney damage or even leading to death.

Patients expect hospitals to protect their safety and privacy. A 2025 survey by HealthCare IT Today revealed that 78% of patients would avoid a hospital linked to a MEDJACK incident, fearing compromised care (Miller). Public trust eroding from healthcare would be catastrophic as a significant percentage of people would neglect receiving medical care. On the legal side a single breach can trigger millions in HIPAA fines, lawsuits, and recovery costs. For example, after a 2024 MEDJACK attack exposed 500,000 records, a Texas hospital system paid $3.8 million in penalties and saw a 15% drop in elective surgeries due to reputational damage (Miller).

A CISO's Roadmap to Mitigating MEDJACK

As a Chief Information Security Officer, tackling medical device hijacking requires a blend of technical rigor and creative problem-solving. Let's start here with the basics: isolation. Picture a hospital network as a busy city. Just as you'd separate power plants from residential zones, medical devices like MRI machines and ventilators need their own secure neighborhoods. By carving out dedicated network segments say, a VLAN that's walled off from general Wi-Fi and guest networks, we can contain threats. If a hacker breaches an infusion pump, they'll hit a dead end instead of waltzing into patient records or billing systems. This isn't just theory either; the FDA's 2024 guidelines explicitly recommend segmentation for high-risk devices, and clinics that adopt it see fewer ransomware domino effects.

Isolation alone isn't enough. Medical devices are quirky; they run along on outdated code and rarely raise alarms when something's off. That's why hospitals need security tools that "listen" to device behavior. Imagine a nurse notices a CT scanner taking twice as long to boot up. Is it a glitch, or is malware quietly siphoning data? Platforms like Darktrace or Medigate act as digital detectives, spotting patterns humans miss or don't look for. For instance, if an EKG machine suddenly starts pinging servers in a country the hospital doesn't operate in, the system flags it instantly. These tools aren't perfect, but they buy time to investigate before a minor anomaly becomes a full-blown breach.

None of this works without cooperation. Device manufacturers hold many of the keys, like firmware updates and vulnerability patches. Too often, hospitals and vendors operate in silos. Bridging that gap is critical. Some manufacturers now offer “security-as-a-service” subscriptions, providing regular tune-ups for devices still in warranty. For older machines gathering dust in storage closets? Virtual patching can act as a Band-Aid, shielding known flaws through next-gen firewalls. And when all else fails, it’s time to negotiate trade-in deals. A hospital in Minneapolis recently swapped 200 outdated insulin pumps for newer models after haggling with the manufacturer, a win for both security and patient care (Kelly).

Then there’s the human factor. A zero-trust mindset ensures no one gets a free pass, not even trusted staff. Multi-factor authentication (think fingerprint scans paired with physical badges) keeps unauthorized users out, while session recording keeps privileged accounts honest. Biomedical engineers, for example, might only get access to MRI software during scheduled maintenance windows, reducing the attack surface.

Finally, assume the worst will happen. A robust incident response plan isn’t just a PDF buried in a shared drive, it’s a living document. Pre-drafted patient notifications, partnerships with forensic experts, and quarterly “fire drills” ensure that when a device is compromised, the team isn’t scrambling. During a 2024 attack on a Boston ICU, staff restored ventilator operations in under two hours because they’d rehearsed the exact scenario. Preparation turns panic into procedure (Abelson).

Conclusion

Medical device hijacking represents a perfect storm: aging technology, sophisticated attackers, and high-stakes environments. However, proactive measures can turn the tide. By isolating devices, adopting intelligent monitoring, and fostering collaboration between IT teams and manufacturers, hospitals can safeguard both patient lives and their own futures. The goal isn’t just compliance, it’s ensuring that every IV pump, defibrillator, and imaging system remains a tool for healing, not harm.

References

- Abelson, R., & Creswell, J. (2024, March 5). *Cyberattack paralyzes the largest U.S. health care payment system*. The New York Times. https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html
- Healthcare Cybersecurity Alliance. (2023). *2023 national hospital device security survey*.
- Kelly, S. (2024, October 7). *Medtronic recalls minimed insulin pumps for reduced battery life*. MedTech Dive. https://www.medtechdive.com/news/Medtronic-Minimed-insulin-pumps-recall-battery-life/729019/
- Miller, G. (2024, December 20). *Healthcare Cybersecurity – 2025 health IT predictions: Healthcare it Today*. Healthcare IT Today | Fresh, Daily, Practical Healthcare IT Insights. https://www.healthcareittoday.com/2024/12/26/healthcare-cybersecurity-2025-health-it-predictions/
- TrapX. (2018). *Medical device hijacking: MEDJACK.4 investigative report* (Report No. MEDJACK-2018). TrapX Research Labs.