Testimony of Dr. Christian Dameff, MD

Co-director of the UCSD Center
for Healthcare Cybersecurity

"Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices"

Before the Committee on Energy and Commerce Subcommittee on Oversight and Investigations

U.S. House of Representatives

April 1st, 2025
Washington, DC

Introduction

Chairman Guthrie, Chairman Palmer, and Ranking Member Pallone, distinguished members of the subcommittee, thank you for the opportunity to testify today about the cyber threats legacy medical devices pose to our great nation. My name is Dr. Christian Dameff and I am a practicing physician. I train medical students and resident doctors as an assistant professor of Emergency Medicine at UC San Diego. I am a little different than your typical emergency medicine doc, however. I am also a hacker, and following my graduation from fellowship was appointed Medical Director of Cybersecurity at UC San Diego Health, the first such position in the nation. I now conduct research on the patient safety impacts of cyberattacks as co-director of the UC San Diego Center for Healthcare Cybersecurity. I also am the co-principal investigator of the Healthcare Ransomware Response and Resilience Program, a two year research effort funded by the Advanced Research Projects Agency for Health (ARPA-H) to revolutionize hospital ransomware detection, and prototype advanced rapidly deployable replacement systems to hospitals under attack, so that they can continue to safely treat patients, even as the “normal” hospital network is being fixed.

Clinical Practice & Medical Devices

Over my 15 years of medical training and practice I have treated thousands of patients in over a dozen healthcare systems. I have worked at large academic medical centers, and small, rural hospitals. Across all healthcare settings, I know this to be true: medical devices are miraculous. Doctors and nurses use them every day to restart stopped hearts, deliver life-saving medicine, and precisely target disease. Over the

years, as we have innovated increasingly powerful healthcare technologies, medical devices, like many other patient care tools, have become connected to networks and the wider Internet.

This capability benefits clinicians in a number of ways- we can collect more data from our patients, allowing us to make better, more personalized medical decisions. We can monitor therapies being delivered out of the hospital, allowing for patients to receive care in the comfort of their home and helping to decrease healthcare costs. We can update these devices remotely, avoiding manual effort, saving patients from cumbersome appointments and providing new functionality for these devices.

The incredible benefits medical devices bring also come with costs. At their core, modern medical devices are computers and this means that there will unavoidably be flaws in code. When flaws in code are exposed to the wider world, cybersecurity threats arise.

Our patients depend on millions of medical devices- many of them aging, machines- to deliver life-saving care. The cybersecurity of our legacy medical devices thus becomes a literal matter of life and death.

Legacy Medical Device Blind Spots

The first step to solving any public health challenge is to understand the extent of the problem. The epidemiology of disease is well known- tracking trauma or counting cancers are hard but realistic tasks. The truth when it comes to the cybersecurity of legacy medical devices is that we lack many of the basic statistics needed to understand the magnitude of the threat. Legacy devices are ubiquitous across our

healthcare infrastructure but how many- which types- how secure- or not- these are all open questions existing in a vacuum of data.

No regional or national medical device inventory exists, and current assessments of the scope of the problem rely on expert opinion or limited biased data sources. Many hospitals themselves lack an internal inventory of their own medical devices, and struggle to understand the attack surface within their own four walls. Compounding this problem is that legacy medical devices that still function are not decommissioned, they are resold on the secondary market where the next healthcare provider assumes the cyber risk, and these “next” healthcare providers are often under-resourced, poorer hospitals that can’t afford to buy new. We currently don't have the capability to determine at a national scale how many and where the legacy medical devices are. Such is the case with Contec and the next dozen devices we find with significant vulnerabilities. No one knows how many CMS8000s there are in U.S. hospitals, or where they are.

The U.S. Food and Drug Administration has done a tremendous job over the last 12 years of improving the cybersecurity of medical devices across the lifecycle. Devices coming on to the market today are significantly more secure than those prior- and that is the result of intentional design and guidance. However, it is critical to understand that cybersecurity is not a solvable problem. Cybersecurity is a dynamic and ever evolving game of cat and mouse. Attack methods of the past have waned with improved defenses only to be reinvented to exploit new categories of vulnerabilities in an ever-raging virtual arms race. The modern medical devices of today are the legacy medical

devices of tomorrow and this paradigm is unlikely to change.

Broad Impacts

While the scope of the legacy medical device problem is unknown, the potential for patient safety impact when devices are compromised is crystal clear. Vulnerable legacy medical devices pose several significant risks to safe and secure healthcare delivery.

Although to my knowledge no medical device has been publicly confirmed as the first point of entry for a ransomware attack, legacy medical devices reside on sensitive hospital networks and the potential for cross-infection is high, meaning that when a hospital network is attacked, it's highly likely that medical devices will become collateral damage.

As ransomware and other cyber threats spread across a network, the likelihood of lost connectivity and disruption skyrockets. When doctors and nurses are not able to utilize network-dependent computers and medical devices, patient care suffers. A growing body of literature highlights the effects ransomware can exert over an entire region. Our research has demonstrated huge spikes in emergency department patient volumes, prolonged wait times, record high ambulance diversions, and worse outcomes from cardiac arrest when ransomware attacks occur in *neighboring* hospitals- the magnitude of impact on infected hospitals is likely even higher. The "cyber blast radius" occurring when one hospital is hit is a ripple effect impacting care across an entire geographic region.

A more ominous scenario arises if adversaries one day deliberately target specific medical devices. While such an event has not yet come to pass, the potential for sophisticated, focused attacks on highly used, highly impactful medical devices could result in widespread catastrophe. Attacks on the most commonly used infusion pumps, laboratory systems, or imaging devices- or on the cloud computing infrastructure such devices increasingly rely on- could prove catastrophic.

The simple reason for this is that medical devices are critical to providing the best care in a number of time-sensitive emergencies. When patients are fighting deadly infection, hemorrhaging from blunt trauma, or suffering from a massive heart attack, minutes - sometimes even seconds- matter. Just as CT scanners are critical for diagnosing life-threatening strokes and infusion pumps are essential to delivering precise amounts of medicine to premature babies, thousands of legacy medical devices are used in hundreds of critical clinical workflows. When doctors and nurses are not able to access these tools, patients are harmed.

Rural & Critical Access

Rural and critical access hospitals provide critically needed healthcare to local communities across the country, allowing many of our fellow citizens the chance to live healthy, productive lives. The financial and operational stress such hospitals are currently under is hard to overstate. Many such facilities are unable to invest in the latest generation of medical devices- and some may be using legacy devices no longer supported by their original manufacturer. I have personally witnessed a hospital system struggling to fix an old CT scanner and ultimately resorting to purchasing spare parts off

Ebay because the cost of a new scanner is prohibitive. The ability to replace aging- but still functional- medical devices to lessen cybersecurity risk is not a luxury many hospitals have.

Financial considerations aside, many rural and critical access hospitals also lack the necessary technical expertise needed to both mitigate device-related cybersecurity risks and more broadly defend fragile hospital networks from sophisticated cyber criminals and state actors. The unique combination of cybersecurity ability and biomedical engineering talent needed to properly deploy, proactively patch and continuously protect legacy devices is scarce even in urban, heavily populated regions. Healthcare cybersecurity professionals are a particularly rare breed amongst the larger cybersecurity workforce- itself too small a pool to meet our nation's growing needs.

Entrenchment

I hope to have illustrated that legacy medical device cybersecurity is a complex, multidimensional problem requiring our best efforts to mitigate, if not entirely solve. We face a number of obstacles in doing so- and I wish to highlight one of the main drivers of this problem- failures at the level of process and people.

Creation of cybersecurity risk in medical devices can occur at many points in the device lifecycle- from design to deployment to discontinuation- and may result from the actions of several different stakeholders. For example, medical device manufacturers may design devices using insecure software libraries or may fail to timely patch discovered vulnerabilities once devices are on the market. Hospitals may choose to procure less secure devices or fail to deploy devices securely by turning off certain

settings in an effort to facilitate installation. Cybersecurity professionals may not maintain accurate device inventories (you can’t defend what you don't know you have), lack the capability to monitor devices for signs of compromise, or fail to timely patch devices to prevent attacks. A single point of failure across any of these domains with any of these stakeholders can prove fatal, if the end result is a vulnerable legacy medical device that is exploited by a cyber threat.

Device manufacturers may be best positioned to raise the baseline cybersecurity of these devices as they are the principal engineers and possess the technical information necessary to implement secure-by-design practices and techniques, but unfortunately, device manufacturers have historically engaged a reactionary approach to legacy medical devices, releasing patches, operating system updates, or end user guidance only after a problem is identified by a third party cybersecurity researcher, hacker, or adversary. In addition, it is not enough for devices to be secure sitting in a box on the hospital’s loading dock--they must be deployed and maintained securely--often in partnership with the manufacturer--by the hospital, and many hospitals, as previously discussed, still struggle to find the people, resources, and time to do so.

Recommendations

Despite understanding that improving the cybersecurity resiliency of legacy medical devices will remain a never-ending challenge, there are many important and necessary steps we must take as a nation to address this threat. I respectfully offer three recommendations for your consideration.

National Healthcare Dependency Mapping

Strategic cyber defence of our critical healthcare infrastructure requires identifying weak points in hardware, software, vendors, supply chains, cloud computing, and networks. No entity, whether commercial or governmental, currently has visibility on healthcare assets across the entire sector. How can we defend hospitals against malicious hackers and highly skilled state actors when we ourselves lack even a rudimentary understanding of the myriad interconnections and dependencies that sustain the overall system? I support the important work led by the Health Sector Coordinating Council to map healthcare's dependencies and associated sector risk.

Remove Barriers to Security Research

The progress made over the last decade on improving baseline medical device security after concerted efforts by stakeholders including the FDA and medical device manufacturers is commendable. Credit must also be given to the seminal work of ethical hackers and security researchers who first demonstrated the existence and technical proof-of-concept of medical device cybersecurity exploits. From early work on pacemaker and patient monitor security to investigations of insulin and infusion pumps, advancements in device cybersecurity first occurred when curious researchers became concerned with the cyber-safety of life-saving devices. Efforts to continue to make devices available to the security research community should be encouraged. Legal protections for ethical hackers and security researchers acting in good faith and using coordinated disclosure practices should be strengthened, including making permanent current DMCA exemptions related to medical device cybersecurity research to enable

exactly the kinds of discoveries that have led to findings like the Contec vulnerability and others.

Empower People, Reduce Human Error: Build and Automate Resilient Systems

As we have established, legacy medical devices and other healthcare cybersecurity challenges arise from systemic challenges at the people and process level. To prevent cybersecurity failure we must undertake new approaches and develop new technologies that reduce dependency on fallible, human designed hardware and code. We must also scale solutions in a way that acknowledges the lack of resources, workforce, and skillset that plague many of the most vulnerable hospitals.

The enormous effort required to not just respond to known vulnerabilities but proactively discover new threats and patch them at scale is hard to comprehend. Government leadership in the form of evidence based policy development and research support, coupled with innovative technologic solutions from industry and academia may provide the force multiplier needed to surmount these existing deficiencies of resources, workflow, and skillset.

The Universal Patching and Remediation for Autonomous Defense (UPGRADE) program created by the Advanced Projects Agency for Health (ARPA-H) provides one such example of a next-generation approach to legacy medical device cybersecurity. By innovating new ways for hospitals to monitor networks and devices, rapidly identify vulnerabilities, automatically develop patches, and deploy patches at scale, UPGRADE seeks to develop new tools for hospitals to protect themselves and their patients . If successful, technologies from this program may transform how we approach medical

device cybersecurity- revolutionizing the current manual, mistake-prone, human dependent status quo.

Conclusion

Legacy medical device cybersecurity vulnerabilities threaten our ability to deliver care to our patients when it matters most, but we can make progress on this pressing challenge. I applaud the committee's leadership on this critical issue, am optimistic that we can improve cyber resilience in healthcare, and sincerely thank you for the opportunity to share my perspective and recommendations.