A TOOL IN MEDICAL DEVICE CYBERSECURITY

SECTION I: STATE OF THE INDUSTRY

DRAFT FDA PREMARKET CYBERSECURITY GUIDANCE RELEASED OCTOBER 2018

The draft guidance released by the FDA solidifies a tiered risk-based approach for device vendors to design security into their devices. The new premarket guidance emphasizes these five key points:

- Devices should make extensive use of encryption to keep data private
- Digital signatures should be used to verify authenticity of devices, data, and instructions
- Devices should be designed in a way that anticipates regular, routine cybersecurity patches
- User authentication needs to be secure and robust
- Devices should be able to alert users when a cybersecurity breach occurs

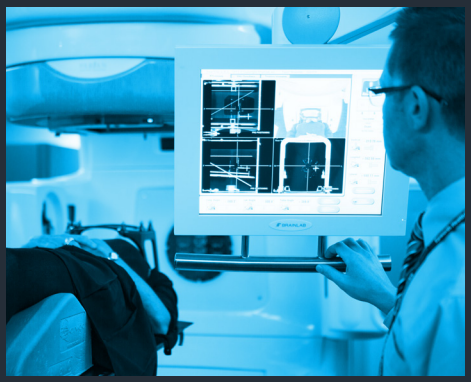
VULNERABILITY DISCLOSURES COVER A SUBSET OF CYBERSECURITY RISKS IN THE ECOSYSTEM

In reviewing all vulnerabilities disclosed between October 4, 2013 - November 1, 2018, we noticed disclosed vulnerabilities **related to only 16% of the NIST-CSF subcategorie**s. (see "Appendix A" for details). The lack of representation of the majority of NIST-CSF sub-categories has two possible explanations. The truth likely lies somewhere between the two.

1. There are no devices with vulnerabilities associated with 97 of the subcategories included in the NIST-CSF guidance
2. Vulnerabilities related to 97 of the 108 subcategories have yet to be reported or identified for medical devices

SECTION II: CYBERSECURITY DOES NOT HAVE A SILVER BULLET

As a security buyer, you may have heard rumors of 'one-stop solutions' and been subsequently disappointed during due diligence. Medical device cybersecurity is complicated, requiring technical and procedural actions by multiple parts of the ecosystem. There is never going to be a product that will guarantee 100% security. Instead, tools are a part of an overall security strategy.



MedCrypt is the software solution that equips device vendors to address critical HDO and FDA cybersecurity requirements with a few lines of code.

MedCrypt's healthcare-first approach solves a specific set of cybersecurity requirements that would have prevented 79% of vulnerabilities disclosed.

Our product makes it fast and easy for software engineers to implement cryptography, without building an entire framework from scratch. Monitoring MedCrypt-enabled devices remotely allows us to detect intrusion, and generate forensic data in the event of a breach. Our ability to detect abnormal behavior stems from our healthcare-specific device behavior data, which spans multiple classes and manufacturers of devices. MedCrypt makes it easy to implement features covering each of the FDA's premarket cybersecurity guidance requirements.

94% MEDCRYPT ADDRESSES NEARLY EVERY PRODUCT INTERVENTION IN THE DRAFT FDA PREMARKET CYBERSECURITY GUIDANCE

Of the 50 design features and cybersecurity design controls described in the draft premarket guidance, we categorized those which can be addressed through the implementation of a product or a process (see here for details). **MedCrypt addresses 16 of the 17 product-related requirements.** Of the **23 process recommendations, MedCrypt supports 10.** The remaining 10 design features include nine architecture decisions a vendor must make, and one that is a non-engineering requirement. **MedCrypt addresses 94% of the premarket guidance's feature and process requirements.**

80% MEDCRYPT ADDRESSES 80% OF POSTMARKET GUIDANCE

Of the 108 NIST-subcategories recommended by the FDA's postmarket guidance, 30 require a technical intervention (28% of the framework). **MedCrypt covers 80% of the technical NIST-subcategories** (see here for details). MedCrypt brings cryptography into various aspects of medical device software and firmware, without a major engineering effort.

79% MEDCRYPT COULD HAVE PREVENTED 79% OF THE DEVICE VULNERABILITIES DISCLOSED

The root causes for vulnerabilities disclosed over the last five years by medical device vendors was reviewed to confirm how MedCrypt could have addressed these vulnerabilities. **107 of the 136 vulnerabilities disclosed could have been addressed** by one or more MedCrypt functions.

THREAT SHARING CAN IMPROVE WITH THIRD PARTY PARTNERSHIP

Empirically[1] beneficial, and expected per the latest FDA premarket cybersecurity guidance, industry wide threat sharing would welcome a new level of maturity. As of October 2018, only seven of the top 30 device vendors have met the challenge to actively disclose vulnerabilities. There are many possible reasons other top vendors have yet to disclose a vulnerability, including the logistical challenges of coordinated vulnerability disclosure, identifying and sharing engineering technical details and the difficulty of completing all of this in a timely fashion. The third-party reporting MedCrypt offers analyzes metadata for threat sharing not only across vendors (as required by the FDA), but also across products within the same organization.

[1] C. Kamhoua, A. Martin, D. K. Tosh, K. A. Kwiat, C. Heitzenrater and S. Sengupta, "Cyber-Threats Information Sharing in Cloud Computing: A Game Theoretic Approach," 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, 2015, pp. 382-389.

SECTION III: MEDCRYPT FEATURES AND FUNCTIONS

With just a few lines of code, MedCrypt can be installed on devices ranging from embedded medical devices to large radiation therapy devices. Using a single patchable library makes ongoing security maintenance manageable.

ENCRYPTION

MedCrypt facilitates the provisioning of unique cryptography key pairs, and supports the use of third-party hardware security modules and PKI systems. Sensitive data and/or commands can be easily encrypted at the application layer, preventing exposure of data and creating redundancy against unknown network security controls.

DIGITAL SIGNATURES

MedCrypt cyptographically signs all commands to enforce communication and/or configuration authentication. Using MedCrypt means the cryptography algorithm can be changed and patched overtime as vulnerabilities are found.

MONITOR DEVICE BEHAVIOR

Devices send on-going metadata (without any sensitive PHI) to enable real-time device monitoring. Monitoring device metadata will "baseline" device class behavior, allowing for potential intrusion detection, threat sharing within a device vendor and vendor-neutral threat sharing (to ICS-CERT or similar).

PUBLISH A CYBERSECURITY BILL OF MATERIALS

MedCrypt tracks versions of its software and component open source libraries to specific devices. Users can also import lists of other component software libraries to be tracked within MedCrypt. This allows us to dynamically generate a SBOM for any MedCrypt-enabled device.

APPENDIX A

The data extracted from the ICS-CERT Advisory Database, including details on advisories and MedCrypt coverage are found here and is summarized in the table below.

NIST-CSF Subcategory	10/2013 - 12/28/2016	12/29/2016 - 11/01/2018	How MedCrypt would have helped
None Noted	1	3	Detective monitoring of anomalous elevated access
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed		1	Detective monitoring of a device connects to a different access point
DE.CM-1: The network is monitored to detect potential cybersecurity events		2	Detective monitoring of a device connects to a different access point
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events			
DE.CM-4: Malicious code is detected	2	3	Port monitoring and encryption on communications inhibit devious updates from being installed
DE.CM-5: Unauthorized mobile code is detected			
ID.RA-3: Threats, both internal and external, are identified and documented	1	2	Code vulnerabilities are diminished through layered security in communication encryption
PR.DS-1: Data-at-rest is protected	3	5	Encryption of data through MedCrypt library
PR.DS-2: Data-in-transit is protected	7	6	Encryption of data through MedCrypt library
PR.DS-4: Adequate capacity to ensure availability is maintained	2	13	Excessive capacity constraints beyond normal behavior are identified through monitoring
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity		2	Cyptographic signatures of data and commands
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	4	10	Keys issued using MedCrypt restrict endpoint communication
PR.AC-2: Physical access to assets is managed and protected			
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	1	4	Architecting limited endpoint communication
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	15	37	Key provisioning and management for endpoints
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	8	16	Monitoring and alerting based on deviations in endpoint behavior
PR.PT-2: Removable media is protected and its use restricted according to policy		1	Modified code injection through removable media would be detected by monitoring
PR.PT-4: Communications and control networks are protected		3	Unintended connectivity to VPN would be identified through monitoring

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer.

Thank you.
Mike Kijewski, CEO
mike@medcrypt.co