A PATIENT SAFETY APPROACH FOR ASSESSING MEDICAL DEVICE VULNERABILITIES

With medical devices being increasingly network-connected, we leveraged our collective expertise in medical device security and clinical risk management, to provide a holistic analysis of vulnerabilities in the medical device space through the assessment of clinical case studies using quantitative analytics, and a discussion of incident prevention recommendations.

AUTHORS

Dr. Saif Abed
Director of Cybersecurity Advisory Services,
The AbedGraham Group

Dr. Gabriel Ma
Senior Clinical Strategist,
The AbedGraham Group

Vidya Murthy
VP Operations,
MedCrypt

Axel Wirth
Chief Security Strategist,
MedCrypt

The AbedGraham Group
Clinically Optimized Success

medcrypt

CONNECTED MEDICAL DEVICES

Medical devices were initially network-connected for device maintenance. Network access allowed vendors to remotely monitor their devices to ensure optimal performance (including rolling out software updates).

This technical optimization quickly became the primary reason for medical devices to be network connected rather than for clinical data sharing or functionality. This resulted in the creation of data silos and poor interoperability between medical systems. In response, medical device vendors started to address the need for smoother clinical workflows by improving the connectivity between devices and clinical systems to enhance sharing of medical information between systems.

The growing digitalization (introduction of digital systems) and digitization (increasing volumes of digital data) has had a profound impact on healthcare's cybersecurity posture. In combination, these trends of increasing external (vendor) and internal (clinical data) connectivity have increased the collective exposure of our medical device ecosystem and has put them at risk of compromise by increasingly targeted and sophisticated cyber adversaries.

RISKS OF INCREASED CONNECTIVITY

Such a substantial footprint of connected medical devices has widened the attack surface area, presenting greater opportunities for hackers (particularly with many medical devices having a weak security posture). Depending on the motives and methods of the attacker there are a range of impacts that could occur. Once the perimeter has been breached the impact could range from a minor disruption to clinical workflow, to suspension of care at scale. The compromise of mission critical systems is increasingly possible in this new, interconnected world of medical devices, IT systems, and third-party cloud services.

The compromise of devices and network infrastructure can have a profound impact on patient safety both directly and indirectly. Most recently, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Department of Health and Human Services (HHS) issued a joint cybersecurity alert warning hospitals of ransomware activity targeting the healthcare and public health sector.[1] The tragic consequences of such attacks can be severe, for example, ransomware induced delay in care delivery is considered a contributor to the tragic death of a patient in Germany.[2]

CLINICAL CONCERNS REGARDING COMPROMISED MEDICAL DEVICES

This has led to a frequently referenced narrative in how compromise of medical devices can result in an imminent risk to patient safety and how such risk could be quantified to help prioritize decisions around mitigation or incident response.

Now whilst this is pertinent for particular devices supporting clinical care at scale, it is important to recognise a majority of medical devices are used to support the isolated care of one individual, often with manual safeguards in place, or with alternative devices nearby.

Therefore, two distinctly different use cases must be assessed:

1. A targeted attack on an individual, specific device with the intent to cause harm to a single patient (essentially an assassination attempt)
2. A scenario where a device is used as an entry point for a wider network attack involving mission critical systems (e.g. PACS, EMR) with the potential to cause harm to many patients.

Use Case 1 is the least likely to occur but has a high potential individual patient safety impact. Use Case 2 has a higher likelihood of occurring, and the level of harm can be significant because of the sheer number of patients that are impacted cumulatively (similar to the effect of a ransomware attack).

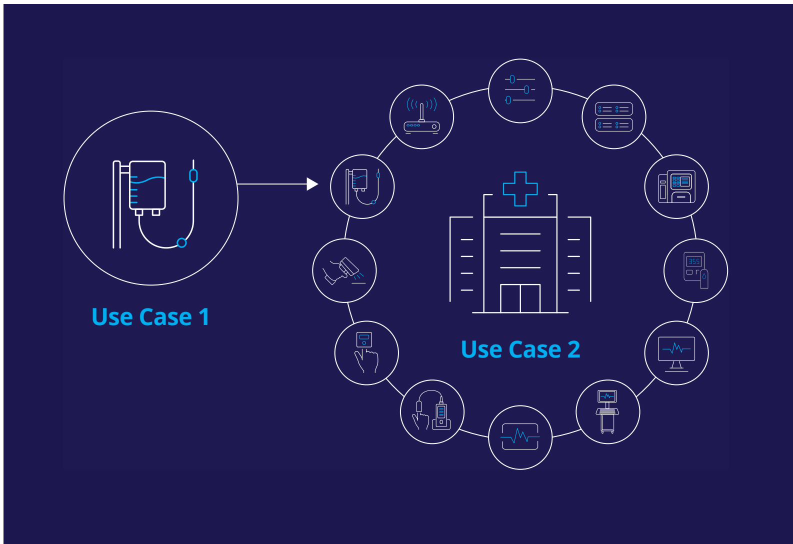
It has been stipulated (and cases have been documented)[3] that the most likely associated risk for these devices is as a point of entry for attackers to establish preparations for future larger scale attacks. Meaning the weak device serves as a beachhead for an attack on the larger clinical and business system environment.

REAL-WORLD IMPACT

Responding to newly discovered software vulnerabilities is not new to healthcare providers, but the frequency of having to do so has gone up dramatically.

To effectively respond healthcare providers must first consult their asset inventory to identify potentially affected devices, assess whether the vulnerability in a given device and implementation would actually be exploitable, and then mitigate it based on risk to patient-safety and other risk parameters. In other words, an impossible task to perform given the quantity and location of devices, complexity of the device ecosystem and technical limitation on what providers' can manipulate.

What has been new about some of these recent vulnerabilities, such as the URGENT/11, Ripple20, or BlueKeep, is their complexity (some including several separate vulnerabilities), their prevalence (e.g., in a widely-used third-party operating system or network stack), and their historic distribution (present for many past generations of a given software). This makes it almost impossible for healthcare providers to



a) understand if and how a given device may be affected, and b) how to mitigate the vulnerability. In other words, for many the barrage of discoveries and disclosures within a short time frame felt like one fire drill after the other. But since everything was a priority, nothing was a priority. This type of vulnerability prevents focusing on the truly relevant and critical risks.

URGENT/11 and Ripple20 are sets of vulnerabilities that affect different TCP/IP stacks which have been used across a high volume of IoT devices for decades, but it was the applicability to medical devices that raised patient safety concerns.

BlueKeep is a wormable flaw affecting a range of devices running one of several generations of vulnerable Windows operating systems and therefore affected a wide range of assets used in healthcare ranging from medical devices to desktop workstations.

Despite these concerns, attacks that impact the availability of medical devices can be perceived as less impactful than initially imagined (and as often portraited in the press) because:

1. The malfunction of medical devices could be mitigated by interventions from supervising clinicians,
2. Affected medical devices could be readily replaced by alternative devices (often on hand and close by),
3. Attacks to isolated devices would affect individual patients only and would not require the replacement of high volumes of devices (limiting the impact to large cohorts of patients).

Compared to that, attacks impacting device integrity would be more complex to carry out and require more in-depth knowledge of proprietary systems and medical workflows to achieve a successful degree of disruption (e.g., altered readings from a medical device would be most commonly interpreted by a clinician as erroneous and a sign of malfunction rather than a true value pertaining to the patient to be acted on).

METHODOLOGY & USE CASE(S)

In order to better demonstrate the cybersecurity risks associated with connected medical devices within the hospital environment, The AbedGraham Group and MedCrypt have partnered together to review a specific two-part use case.

Use Case 1 will analyze the risks associated with a post-surgical patient located on the High Dependency Unit (HDU) with an infusion pump compromised by the Ripple20 vulnerability.

Use Case 2 will analyze the risks within a wider departmental context when taking into considering the range of other connected IoT devices involved in the provision of care to multiple patients in the same HDU.

The goal of these use cases is to contextualise the associated risks of a solitary medical device (taken in isolation), against the backdrop of a more pragmatic scenario involving multiple devices with a diverse range of vulnerabilities present.

USE CASE ANALYSIS

In the following, we share a holistic analysis of the associated risks, contrasting both a qualitative and quantitative assessment of the risks associated with both scenarios.

Qualitative Analysis

The qualitative assessment will involve a technical analysis of the risks by the MedCrypt team.

Quantitative Analysis

The quantitative assessment involves the use of the AbedGraham Group's clinical security analytics platform – [CCOM^2]. This platform contextually analyzes, ranks and visualizes each endpoint based on the risks they present to a health system clinically, organizationally, financially and in terms of regulatory compliance using a standardised 1-12 point scale. This is achieved using algorithmic models that take into account a broad range of behavioural attributes of network endpoints based on their functional behaviour across clinical workflows and associated interdependencies. In doing so a granular asset profile can be determined and different types of attacks can be modelled based on the detected vulnerabilities allowing the platform to determine the severity of any potential patient safety risks and their scalability.

The four key thematic impact metrics are defined as follows:

Clinical Risk

Pertains to the potential severity of patient harm that could occur

Organizational Risk

Pertains to the level of clinical workflow disruption or service shut down that could occur

Financial Risk

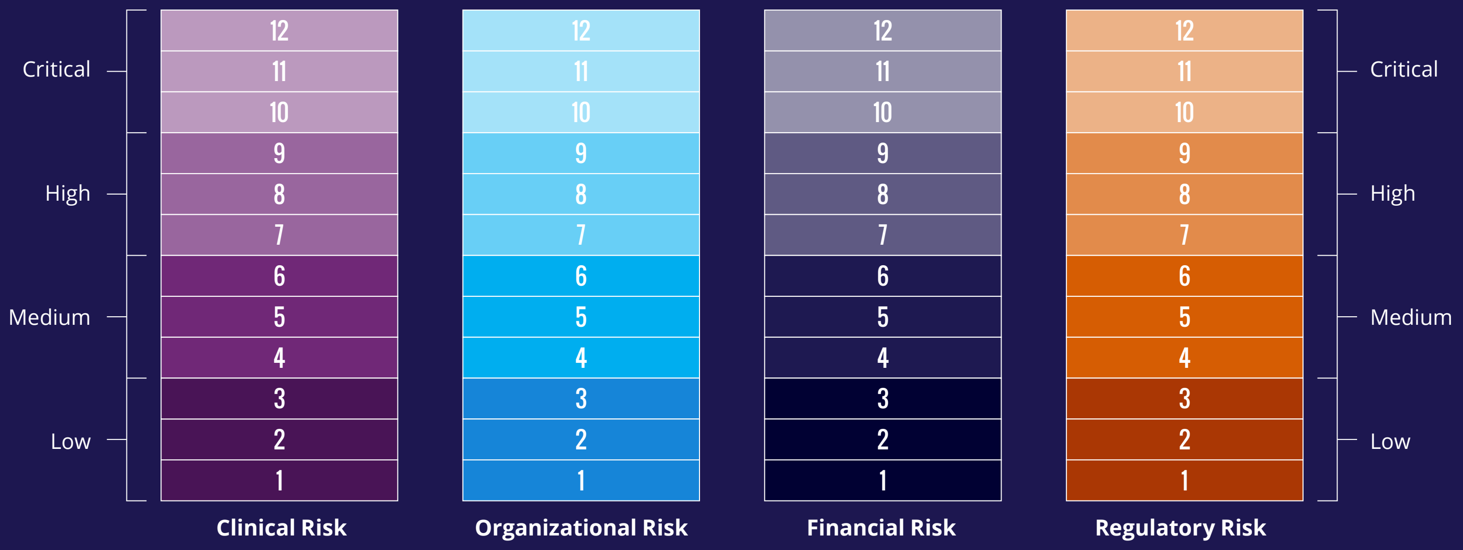
Pertains to the potential level of recovery and regulatory costs, as well as revenue losses that could occur

Regulatory Risk

Pertains to the severity of intervention from regulators following disruption and degree of reputational damage

The patient safety and clinical workflow disruption risk metrics produced can be scaled to provide a total health system risk profile and the insights can ultimately guide any remediation strategies and application of security controls.

[CCOM^2] Remediation Heat Maps



RESULTS - USE CASE 1: INFUSION PUMP

Use Case 1: What is the risk associated with one of the most severe Ripple20 vulnerabilities found to be present on an active infusion pump providing pain relief to a post -operative surgical patient located on the High Dependency Unit (HDU)?

Qualitative Results

The identified example of Ripple20 is actually a collection of 19 individual vulnerabilities (identified as CVE-2020-11896 through CVE-2020-11914) associated with the Treck, Inc. TCP/IP network stack. As documented by the U.S. ICS-CERT (Industrial Control Systems - Cyber Emergency Response Team), it affects a set of network protocols including IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4, and ARP.[4]

Collectively, Ripple20 has been assigned a CVSS v3[5] score of 10.0 (highest possible), however, the individual 19 vulnerabilities under the Ripple20 umbrella have been assigned scores in the range of 3.1 to 10.0. At least one of the vulnerabilities could enable access from outside the network boundaries.

The associated software weaknesses provide the possibility to compromise a system via common exploit techniques like remote code execution, out of bounds read/write, or device memory exploits.

Due to the intrinsic nature of the global software supply chain (and associated security risks),[6] Ripple20 is found in many devices that have been produced for years. It has been estimated that worldwide as many as hundreds of millions of devices could be affected ranging from printers to infusion pumps and impacting industries from aviation over healthcare to utilities.

In that sense, Ripple20's impact is significant due to the large number of individual vulnerabilities and the criticality of several of them, while also the wide use of the underlying software library across the globe and across industries – its discovery had a true "ripple effect".

Treck, Inc. has provided a patch for use by original equipment manufacturers (OEMs) with the Treck stack software version 6.0.1.67 and after. This obviously required that OEMs implement and test the update prior to disseminating the patch to end users who then need to deploy it to individual devices – likely a long, time consuming, and often incomplete process. As a possible mitigation, ICS-CERT advises that operators should minimize network exposure of critical devices, ensuring that devices are not accessible from the Internet unless absolutely essential.

Quantitative Analysis

In this scenario, when using [CCOM^2], an infusion pump with a Ripple20 vulnerability (with a CVSS score of 10, see table 1 in appendix) would give, as expected, a critical clinical risk score of 10/12 as it is involved in the direct provision of clinical care. By being connected to the network, there is always a baseline risk that the device can become a point of entry into the wider network, with high scoring vulnerabilities providing attackers with a diverse range of options to create various types of disruption across the organisation. However, as there is a high degree of variability, following the initial attack on the infusion pump, the baseline risk of such an isolated device combined with its impact on relevant users would be associated with relatively moderate risk in the other organisational (7/12), financial (6/12) and regulatory (6/12) categories resulting in a total score of 7/12.

Key Analysis

Whilst an infusion pump can be involved in the management of multiple patients during its lifetime, it would predominantly be used in the care of one patient at a time during a 24-hour period in HDU. Compromise of this device by exploiting a critical vulnerability therefore could directly and significantly impact the care of a single patient (hence the high clinical risk score). However, it is highly unlikely to cause scalable direct disruption to the care of multiple patients or systems. This is what we describe as an 'n=1' with one type of endpoint where its failure is constrained to an individual patient or workflow. Contrary to that, the failure of an EMR system would affect multiple workflows across multiple patient groups and sites.

In terms of indirect harm, the localised workflow(s) of the nurse(s) responsible for looking after the individual patient could be impacted, with resource and costs required to repair/replace the device, as well as manage the aftermath of any resulting clinical incidents (dependent on what the infusion pump was being used to administer), but it is important to emphasise that this is a highly localised level of disruption.

RESULTS - USE CASE 2: MULTIPLE ENDPOINTS IN HDU

Use Case 2: How does this compare to the wider departmental context when considering the range of other connected IoT devices involved in the provision of care to multiple patients in the same HDU?

Qualitative Results

The Ripple20 vulnerability has previously been discussed under Use Case 1. Since we are reviewing a use case example of a larger system with several different types of endpoints, we need to look at a second sample vulnerability, BlueKeep (CVE-2019-0708).

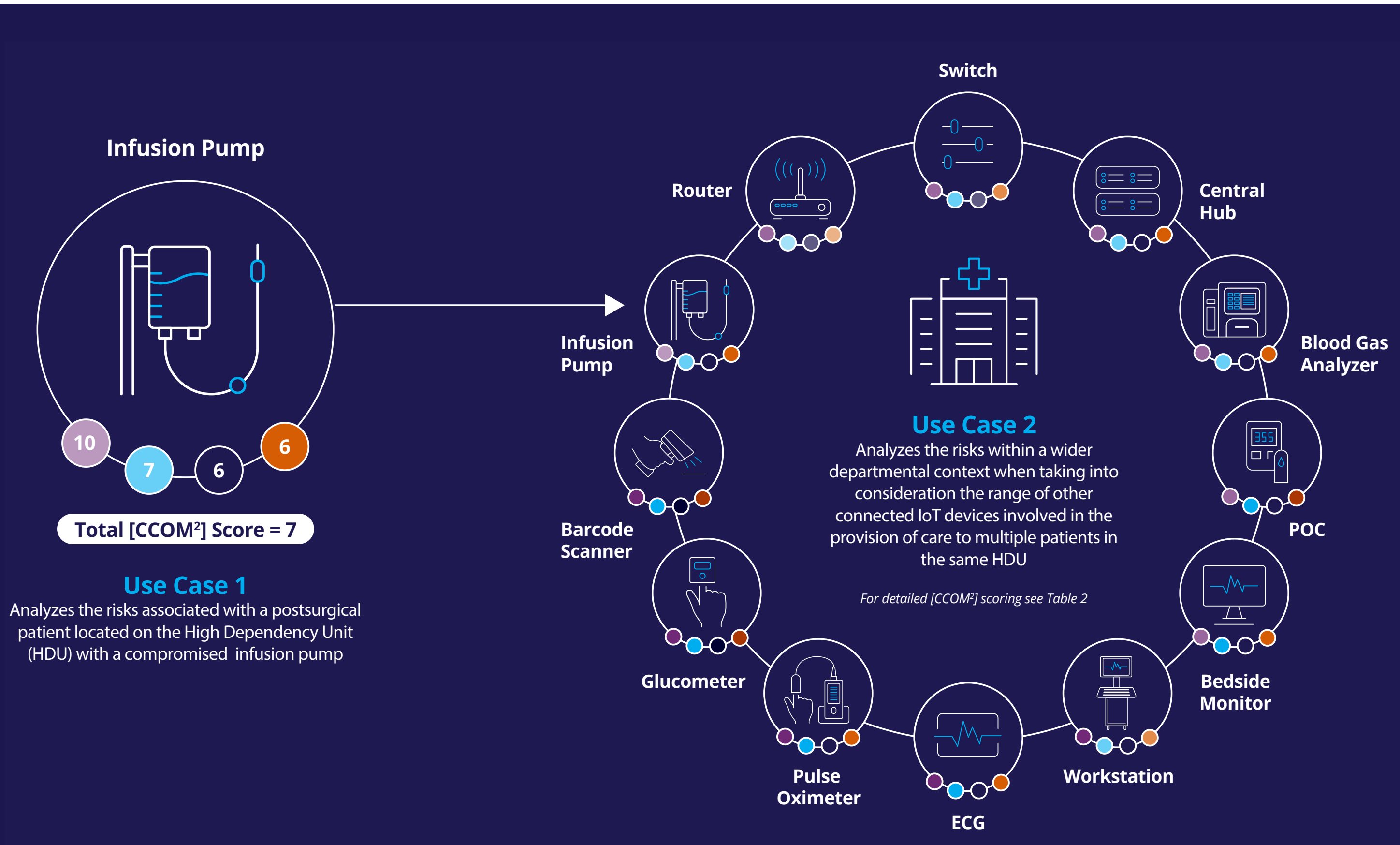
The BlueKeep vulnerability is present in the Remote Desktop Protocol (RDP) of several generations of the Microsoft Windows operating system (Windows 2000 / Vista / XP / 7 and Windows Server 2003 / 2008). A vulnerable system can be exploited by an attacker to take control of the system via remote code execution.

An attacker could perform a number of actions: creating accounts with full user rights; viewing, changing, or deleting data; or installing malware. The BlueKeep vulnerability has been given a CVSS 3.x base score of 9.8 (critical),[7] is considered "wormable", and could enable malware to propagate to other systems similar to, for example, the WannaCry malware.

First steps to mitigation include identification of at-risk systems that have RDP enabled, then validate and deploy the provided patches per Microsoft Security Advisory[8] and Customer Guidance for CVE-2019-0708.[9]

Microsoft has also released patches for some OSs that are no longer under support (Windows Vista, Windows XP, and Windows Server 2003).

Where these mitigations can not be implemented or implementation is delayed, the following measures can reduce the risk:



Total [CCOM^2] Score = 7

Use Case 1

Analyzes the risks associated with a postsurgical patient located on the High Dependency Unit (HDU) with a compromised infusion pump

Use Case 2

Analyzes the risks within a wider departmental context when taking into consideration the range of other connected IoT devices involved in the provision of care to multiple patients in the same HDU

For detailed [CCOM^2] scoring see Table 2

- Upgrade no longer supported (end of life) operating systems.
- In general, disable all unnecessary services and specifically RDP.
- Enable Network Level Authentication (exploiting BlueKeep requires an unauthenticated session).
- Block TCP port 3389 at the firewall if possible (unless external RDP sessions are required; does not prevent exploit from inside the network).

The two sample vulnerabilities, Ripple20 and BlueKeep, have very different characteristics and affect organizations in very different ways. BlueKeep is found in several generations of Windows and is prevalent across the enterprise, ranging from traditional IT endpoints (desktops, servers) to medical devices built on the respective OS version. Due to the popularity of Windows it has to be assumed that many exploits (malware and attack tools) have been and will be developed.

Ripple20 on the other hand is mainly found in dedicated purpose systems like medical devices and was introduced via a commonly used network stack. Although less prevalent, the criticality of the target systems and the fact that it includes a number of separate vulnerabilities create their own level of complexity and risk.

Quantitative Results

In this scenario when using [CCOM^2] , for a diverse range of endpoints in HDU (which can include other infusion pumps, patient monitoring peripherals, bedside monitors, diagnostic equipment, IoT hubs, workstations and infrastructure components etc., see table 2 in appendix), with a range of vulnerabilities (a mix of Ripple20 & BlueKeep) present across these devices, a wide variety of scores can be expected (as not all the associated vulnerabilities will have high CVSS scores). As there are likely to be several devices within each device type (we initially had a total of 67 endpoints considered in this use case), in the interests of conciseness only a sample of key devices and their associated [CCOM^2] scores has been shown above to demonstrate the potential variation in final impact metrics.

When compared to the infusion pump in part 1, 27% of the 67 endpoints in our model HDU had the same (or higher) total risk score (≥7/12) including routers, switches, patient monitoring hubs & blood gas analysers. The remaining endpoints had lower total risk scores in part because the selected vulnerabilities associated with these from the Ripple20 suite were less technically severe.

It is important to note that despite devices such as patient monitoring hubs and blood gas analysers having the same total risk score (7/12) as the infusion pump in part 1, they have different COFR constituent scores (such as lower clinical risk scores and higher organisational risk scores) associated with them.

At the same time, although endpoints such as workstations have a lower total risk score (due to the lower clinical risk score), they have the same organisation and financial risk scores with a higher regulatory score than the infusion pump in part 1.

Key Analysis

As the healthcare sector expands its use of technology to optimise productivity and enable greater efficiencies to be made, a key component of this involves smoother integration and connectivity (both within and between providers) across multiple settings. This has, no doubt, been accelerated by the global COVID-19 pandemic. The growth of telemedicine and demand for interoperability means that the number of connected devices, systems, and supporting infrastructure will continue to follow an exponential trajectory, with patients monitored during an inpatient stay and increasingly during transfers back into the community. The increased availability of cloud services and smart phones further enables clinicians to monitor patients remotely (including from home).

This is somewhat reflected in Use Case 2, where a sample of endpoints present in the HDU has highlighted the variation and extent of the associated impact risks. This is particularly prominent where endpoints either are used to support multiple cohorts of patients or are considered parts of mission critical infrastructure that provide access to key clinical systems.

Although there will be a high volume of certain device types in HDU (such as peripheral monitoring devices), similar to the infusion pump in the first use case, such a scenario would not necessarily result in scalable attack in all cases. It is also possible that the spread of vulnerabilities may be mitigated through replacing devices.

This does not mean that these risks should be ignored rather that they need to be considered thematically in terms of outcomes. For example an n=1 device will be lower in terms of scalability but potentially still critical clinically at the individual level. This contrasts with the failure of a PACS server leading to a loss of access to radiological capabilities across a health system which is a high scale, process oriented risk that is more indirect in terms of clinical harm (e.g. loss of diagnostic capabilities leading to delayed patient care and therefore harm contrasting with the pain caused if a pain management infusion pump stops working).

This type of detail encourages the various senior stakeholders to look at risk holistically, and prompts discussion around how to manage the diverse range of endpoints collaboratively when considering remediation.

DISCUSSION AND RECOMMENDATIONS

Prioritise Clinical Risk

We have demonstrated that assessing medical IoT device risks in their true context requires a more complex and sophisticated assessment methodology than purely looking at the CVSS vulnerability score of the individual software components. To address this, we utilized the clinical security analytics platform [CCOM^2], developed by The AbedGraham Group, as an example of how such a comprehensive and holistic approach could be achieved by assessing the risks associated with vulnerabilities through a detailed knowledge of clinical workflows, their interdependencies and scalability. This allows both security and non-technical executives to understand risk based on tangible clinical and business disruption outcomes. Additionally, our findings clearly demonstrate that individual vulnerabilities, when considered in the context of different clinical workflows and their interdependencies, can have profoundly different risk profiles than their CVSS scores would indicate at face value. This can significantly alter how remediation and incident response plans are developed.

When considering medical IoT security moving forward, we recommend that for both healthcare providers and medical IoT manufacturers it is critical to have a means of rapidly and contextually assessing risk beyond applying simple technical metrics. Questions that need to be considered include:

- What are the clinical workflows that are dependent on a device?
- Does failure of a device act as a workflow bottleneck for a health system?
- Does a device affect one or many patients?
- Is the failure of a device associated with morbidity, mortality or both?
- What's the financial impact on a healthcare provider of device failure?
- What's the regulatory impact and reputational damage for manufacturers and providers of device failure?

These are a subset of complex questions that need to be answered at the development stage of products, in order to consider appropriate safeguards, and also as a part of ongoing future vulnerability monitoring and remediation. As manufacturers and healthcare providers increasingly start sharing the burden of risk management, having a means to conduct relevant real time risk analysis is critical. The [CCOM^2] platform is one, automated option to address this.

Be Proactive

In the end, the path forward for the management of medical IoT devices will require a two-pronged approach:

- At the design stage in a device's lifecycle, integrating the appropriate security technology and embedding risk mitigating approaches into the architecture of a device (i.e., a proactive, "shift left" approach to security).
- After deployment in a healthcare setting, identifying vulnerabilities on an ongoing basis and prioritising the most impactful for remediation (i.e., apply a reactive approach to the remaining issues, that have been reduced in number to an acceptable and manageable minimum).

Healthcare organizations that have implemented a reactive security program have already reached an initial milestone, but need to realize that by itself it only incrementally enhances their security posture, especially if this approach is dependent on technical metrics alone. Additionally, a reactive, predominantly network-based security strategy combined with vulnerability mitigation and patching, results in significant costs and resources invested by the HDO. Despite this resource intensiveness there will still be exploitable network weaknesses and there is no guarantee that all attack vectors will be addressed (e.g. protect against USB-based malware). As for patching, we need to ask ourselves the question whether we ever will be able to patch at a rapid and robust enough pace to become secure at a level that's necessary for the criticality of clinical environments. Realistically, the answer is probably 'no' given the rate at which new vulnerabilities are being discovered and the resource constraints most healthcare organizations have.

Therefore, security needs to be implemented as early as possible in the device lifecycle – and that is during the device's design. This is not only the most secure but also the most cost-effective approach when looking at security investment across the entire device life. Manufacturers should consider the risk profile of their IoT devices more granularly and consider potential mitigations such as those offered by MedCrypt. This will sufficiently reduce the reactive part of security response, which then can be combined with a multi-faceted risk prioritization approach, as shown in this paper based on the use of the clinical security analytics platform [CCOM^2].

Regulatory and industry initiatives are driving towards a more reliable and proactive approach to security and are advocating more transparency on device composition (SBOM) and vulnerability disclosure. As a call to action, we, the healthcare industry, need to make a serious effort to participate in these activities, but more important, improve the security posture of our medical devices. This can only happen through a combination of "left -shifting" security investment and a context-aware assessment of what the remaining security risks will be.

References:

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-302a_

[2] AAMI Blog, "Ransomware-Linked Death Hits Close to Home", Sept. 25, 2020, available at: https://aamiblog.org/2020/09/25/axel-wirth-ransomware-linked-death-hits-close-to-home/

[3] http://www.cs.tufts.edu/comp/116/archive/fall2018/smeggitt.pdf

[4] https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01

[5] https://www.first.org/cvss/user-guide

[6] https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

[7] https://nvd.nist.gov/vuln/detail/CVE-2019-0708

[8] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[9] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

ABOUT THE AUTHORS

At the AbedGraham Group, our blend of clinical and technical expertise drawn from our team of physicians and security analysts, means that we are in a unique position to interpret cybersecurity events in the healthcare sector with a specialized focus on patient safety and clinical service disruption. This is particularly relevant when it comes to the increased uptake of connected medical IoT devices.

MedCrypt is a healthcare cybersecurity company that focuses on proactively securing medical devices to ensure that clinical functionality, patient safety, and care delivery are always the highest priority.

The AbedGraham Group
Clinically Optimized Success

The AbedGraham Group is a global healthcare IT and cybersecurity technology group providing clinically led advisory services and analytics solutions for technology companies, government agencies and healthcare providers.

For further details about [CCOM^2] please visit and contact:

Website: www.abedgraham.com
Email: info@abedgraham.com
Twitter: @AbedGraham

medcrypt

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a $5.3 million Series A funding round in May of 2019, bringing the total funds raised to $9.4 million with participation from Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California.

For further details, please visit and contact:

Website: www.medcrypt.com
Email: info@medcrypt.com
Twitter: @MedCrypt

APPENDIX

Quantitative Results Use Case 1

INFUSION PUMP	10	7	6	6	7

Table 1: Use Case Part 1 - Ripple20 [CCOM^2] Analysis and Results

Quantitative Results Use Case 2

DEVICE	CLINICAL RISK	ORGANIZATIONAL RISK	FINANCIAL RISK	REGULATORY RISK	TOTAL
ROUTER	9	10	9	10	9
SWITCH	7	8	7	8	8
CENTRAL HUB	8	9	6	5	7
BLOOD GAS ANALYZER	7	8	6	6	7
POC	7	6	5	4	6
BEDSIDE MONITOR	7	6	5	4	6
WORKSTATION	5	7	6	7	6
INFUSION PUMP	7	5	5	5	5
ECG	5	6	4	4	5
PULSE OXIMETER	5	6	4	4	5
GLUCOMETER	5	5	3	2	4
BARCODE SCANNER	4	4	3	3	3

Table 2: Use Case Part 2 - Ripple20 and BlueKeep [CCOM^2] Analysis and Results