HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 6 • € 22

ISSN = 1377-7629

Cybersecurity: Preventing the Worst-Case Scenario

THE JOURNAL 2022

9 771377 756005 09

Internet of Medical Things: Threats and Recommendations

Alexios Antoniou | Cybersecurity Consultant | KPMG | Cyprus

Internet of Medical Things (IoMT) aims to deliver game-changing benefits to healthcare institutions, patients and society. It supports more accurate diagnoses, improved treatments, and better availability of care. IoMT systems face challenges, such as the security of all the interconnected components. This article aims to present a few vulnerable components and point out recommendations for better security.

Key Points

- Internet of Things (IoT) denotes all electronic devices (apart from traditional computers) that are connected to the internet.
- In 2018, the IoMT market value was $44,5 million and is expected to reach $254.2 million by 2026.
- As with any device connected in the cyber realm, IoMTs are also exposed to threats and cyber-attacks.
- Since some security challenges for IoMT are new and different, an adapted application of measures is necessary.

Internet of Things (IoT) denotes all electronic devices (apart from traditional computers) that are connected to the internet, and their aim is to collect, analyse, and transmit information or respond to remote commands. IoT has been an enabler for many different sectors, such as manufacturing, transportation, utility organisations and healthcare institutions. Internet of Medical Things (IoMT) refers to the ecosystem of advanced digital devices and systems which can collect, transfer and analyse data regarding someone's health condition. IoMT enables the transfer and processing of medical information through a network without human interaction and allows for remote, automated, 24hr healthcare services.

There are different IoMT device categories according to their purpose and their use. In total, there are the following five categories.

1. Fitness Tracking Devices: Used to monitor someone's physical activity. These devices can be wristbands or smartwatches.
2. Clinical Grade Wearable Devices: Used to improve a user's chronic health conditions. These devices can be smart belts that are capable of detecting falls and informing a carer.
3. Monitoring Devices: Used to keep a patient under constant monitoring. It can be a blood glucose monitor.
4. Smart Pills: Used in medication administration compliance. Smart pills are similar to traditional pills, with the only addition being that they have ingestible sensors.
5. Hospital Devices: Used to monitor hospitalised patients. These devices refer to infusion pumps, MRIs, CT scanners and Ultrasound Scanners.

In 2018, the IoMT market value was $44,5 million and is expected to reach $254.2 million by 2026. The four main pillars that contribute to the raised market value are medical devices (32.91%), system and software (31.01%), technology (17.72%) and services (18.36%).

The workflow in the IoMT ecosystem starts with the IoMT devices. These devices, which are equipped with sensors, collect users'/patients' medical data and forward it to cloud services through gateways such as smartphones over wired or wireless network technologies (i.e. Infrared, Bluetooth, Zigbee, Wan etc.). Depending on the underlying communication protocols, encryption methods are used to secure device communication. Upon receiving information, the gateway then needs to transfer it directly to the cloud or to a fog server. A fog server collects data generated by IoMT devices processes, analyses and summarises it before forwarding it to the cloud services. The purpose is to reduce the bulk of information transmitted to the cloud services reducing the communication bandwidth as well as the required cloud storage capacity. When the information arrives at the cloud services, data aggregation, processing, visualisation and knowledge distribution to healthcare professionals take place. In some cases, the cloud services are connected to external applications such as Clinical Decision Support Systems (DSS), which aid clinicians when they have to make complex and tough decisions regarding a patient's medication/therapy.

Secure IoMT device authentication and communication is implemented through enterprise-wide cryptography policies. The number of IoMT devices in a healthcare ecosystem is vast, and manual management of digital identities is impractical. IoMT devices' performance and scalability are essential. The use of an automated machine identity management system will increase efficiency and effectiveness. Such systems offer automatic device registration and de-registration, automatically update device identities and credentials, and support standard-based authorisation. They also reduce the window of exposure when facing a cyber-attack or when responding to a newly announced vulnerability.

The amount of information generated in the IoMT realm is enormous. The application of edge computing technologies has been proposed to address capacity and node communication bandwidth challenges. According to edge computing, nodes with processing capability are installed at the edge of the network, near the physical location of IoMT devices. These edge nodes process the generated data, and only aggregated data sets are forwarded to the cloud. According to Dilibal (2020), edge computing in healthcare could minimise communication latency and data streaming, reduce alarm notification and response delays, and decrease the cost of healthcare monitoring platforms.

IoMT-based solutions have also been proposed to remotely run medical examination tests which are otherwise expensive to carry out. Detection of sleep apnoea is such an example. Sleep apnoea is a potentially serious sleep disorder where breathing stops and starts periodically many times during a night's sleep, affecting the sleep quality and, as a result, the mental, physical and emotional functioning of the patient. Haoyu et al. (2019) proposed a scheme that uses IoMT to detect sleep apnoea incidents in real-time and promptly inform patients and doctors. The system utilises a SpO_2 sensor to monitor blood oxygen levels and heart rate. Data is transferred through a gateway to the cloud for diagnosis and further processing. Tests have proven the proposed scheme to produce at least 97% accurate diagnoses.

As with any device connected in the cyber realm, IoMTs are also exposed to threats and cyber-attacks. Numerous vulnerabilities have been identified and reported for a significant number of devices. Organisations like NIST (National Institute of Standards and Technology) and CISA (Cybersecurity and Infrastructure Security Agency) maintain records on known vulnerabilities, including a detailed description of the problem, threat scoring, affected units, and recommended mitigation actions. This section presents four such cases and critically examines the probable impact on a healthcare institution due to successful exploitation. Vulnerability severities have been assigned by NIST using the Common Vulnerability Scoring System (CVSS) version 3. CVSS's base score takes into account five exploitability metrics (Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), and Scope (S)), capturing how complicated exploitation is. Three additional metrics capture the impact on Confidentiality (C), Integrity (I) and Availability (A). Classification is expressed as a vector of attributes for the eight parameters and a numeric score from 0 to 10. A score of 9.0-10.0 is classified as Critical, 7.0-8.9 as High, 4.0-6.9 as Medium and 0.1-3.9 as Low. A high classification denotes higher risk for which mitigation actions should be prioritised.

A threat actor with access to a vulnerable IoMT device could potentially escalate privileges to admin, modify operating parameters, implement denial of service or gain access to sensitive information

The first vulnerable component is named ExactaMix1200, developed by Baxter, and the affected-vulnerable versions are from 1.1 to 1.5. Compounding, with regards to medical sciences, is the preparation of a custom combination of medication to be administered to a specific patient suffering from a condition that cannot be dealt with commercially available medicines. ExactaMix1200 is an automated compounding system manufactured by Baxter that aims to increase efficiency, accuracy, production levels, and compounding effectiveness. Its primary function is to compound sterile ingredients into a finished product in a single bag. It integrates seamlessly with order entry calculation software as well as pharmacy workflow management software.

According to CISA, ICS Medical Advisory ICSMA-20-170-01 Etxacta Mix 1200 units, versions 1.1, 1.2, 1.3, 1.4 and 1.5 suffer from CVE (Common Vulnerabilities and Exposures) CVE-2020-12016. This CVE has a CVSSv3.0 score of 8.1 (High). The device uses a hard-coded password set by the manufacturer, transmits sensitive data in clear unencoded form, stores data in clear form, allows booting from a live USB, does not restrict non-administrators from changing the start-up script and does not validate input via a port (SMBv1) which can affect control flow of the system.

A Threat Actor (TA) with access to such a device could achieve administrator's privileges, modify operating parameters, implement denial of service and gain access to sensitive information, including Patient Health Information (PHI). This could have a major impact on operations, endanger patients' lives and cause significant financial losses if ransom payment is required. Moreover, an event of such a scale could severely impact patients' confidence in the services provided by the institution.

The second vulnerable component is named Outlook400ES, developed by B.Braun Medical Inc. Outlook400ES is a medical infusion pump that is used to deliver fluids into a patient's body in a controlled manner. The Outlook 400ES system was designed to provide reliable intravenous medication administration and has wireless drug library capabilities to simplify medication composition and control. It supports an open design that enables interconnection with a large number of external vendor applications. According to a security announcement by B. Braun, Outlook 400ES is affected by the following vulnerabilities: CVE-2020-11906 with a score of 5.3 (Medium), and CVE-2020-11903 with a score of 5.0 (Medium).

The combination of the above vulnerabilities may allow a TA to read sensitive information from other memory locations or cause a crash exposing the healthcare facility to disruption of operations, leakage of sensitive patient data and finally to ransomware demands. Such an event could carry a significant impact both on the profits of the institution as well as on customer confidence.

The third vulnerable component is named Volution730, developed by General Electric, and the affected versions are the BT05 and BT08. Volution 730 is an ultrasound station which uses high-frequency sounds to produce an image of a woman's bladder, fallopian tubes, ovaries, uterus and cervix. It is used to monitor pregnancy and to evaluate medical conditions regarding the aforesaid female body organs. According to CISA, this device is affected by vulnerability CVE-2020-25179 with a score of 9.8 (Critical) because it employs unprotected transport of credentials and exposes sensitive system information.

A TA with access to the network to which such a device is connected can log in to the system with privileges comparable to a GE service user account. Sensitive PHI is exposed, arbitrary code can be run on the machine, and PHI can be modified. The TA can use these as leverage towards the healthcare institution imposing their demands for payment to release control of the systems and avoid releasing PHI to the public domain.

The final vulnerable component is named RapidPoint500 and was developed by Siemens. RAPIDPoint 500 is an automated blood analyser. It can test blood gas, electrolytes, glucose, lactate and full CO-oximetry. It supports multiple sample types and can perform hands-free automated sampling to reduce biohazards.

According to an announcement by Siemens, the device is affected by CVE-2018-4845 with a score of 8.8 (High) and CVE-2018-4846 with a score of 7.3 (High). The first CVE allows a remote attacker with credentials to the "Remote View" feature to achieve elevation of privileges, compromising confidentiality, integrity and availability of the system. Exploitation metrics are assigned high values indicating that special skills or user interaction are not required for a successful exploit. The second CVE refers to a factory set account with a hardcoded password, allowing remote control over TCP port 5900. Once again, no special skills or user interaction is required, and device confidentiality, integrity, and availability are compromised.

A TA could effectively control the device, make it inoperable and demand a ransom before releasing it. The impact of an institution relying on such devices to deliver accurate and quick blood analysis results could be critical, as operations may be put on hold until the situation is resolved. Patients may turn to other facilities for their tests, and the institution's brand might be damaged irredeemably.

As has been mentioned, the IoMT components are vulnerable to cyber threats. The whole ecosystem must perform in a safe and secure environment. Security principles that have been studied for many years still apply; however, since some security challenges for IoMT are new and different, an adapted application of measures is necessary.

This article concludes with recommendations to be implemented at procurement, deployment, and management, significantly reducing the attack surface and minimising exposure to cyber-attack threats. During the procurement stage, all devices that run outdated operating systems should be avoided as these devices are no longer supported, and no security updates will be released. Healthcare institutions should opt for manufacturers who apply the 'secure by design' principle, where security is considered and implemented into a product at every development stage. Such devices implement exploitation mitigation techniques like software verification at boot and encryption of data stored or transmitted and will be much more difficult for TAs to exploit. They should also opt for devices supporting control by an automated identity management system and for providers who apply a policy to disclose regularly and promptly any vulnerabilities identified for their devices. Moreover, healthcare institutions should make sure that the devices' vendors will be delivering device security updates at regular intervals covering the whole lifecycle of the product. Finally, it is not recommended to use any devices that are factory programmed with hardcoded, non-unique credentials, as these may be easily exploited by TAs.

During the deployment stage, healthcare institutions should apply the defence in depth principle by using a series of layered security controls so that in case of an attack, the multiple security layers will make accessing sensitive devices or PHI data more difficult. They should also implement security zoning by isolating computer networks that serve different functions so that a TA who gains access to a network can be contained and apply the principle of least privilege, which means that the devices will have access only to data and functions that are needed to complete a required task. Finally, healthcare institutions should make sure that the data storage processes align with regulations, legislations and codes of practice such as the General Data Protection Regulation (GDPR).

When managing the IoMT devices, once again, healthcare institutions should apply the principle of least privilege to operators so that each person will have the minimum privileges required to perform his/her daily tasks. This way, in case of leakage of credentials, the attack surface is much more limited. Further, it is recommended to install an automated identity management system. These systems enforce higher device security, reduce maintenance costs through automated identity management, ensure compliance with security standards and manage secure firmware updates. They also allow for a much quicker response if multiple identities need to be revoked or reworked because of a security incident. Lastly, it is also recommended that healthcare institutions run system security evaluations periodically by utilising the services of companies specialised in the IoMT domain.

Conflict of Interest

None. ■

REFERENCES

All the Research (2020) Global Internet of Medical Things (IoMT) Market – Segment Analysis, Opportunity, Competitive Intelligence, Industry Outlook 2016-2020. Available at https://www.alltheresearch.com/report/166/internet-of-medical-things-market

Alqahtani B, AlNajrani B (2020) A Study of Internet of Things Protocols and Communications. 2nd International Conference on Computer and Information Sciences (ICCIS), 13-15 October. IEEE.

BBraun (2020) B. Braun Statement on Cybersecurity Vulnerability with Ripple20 Communications Software. Available at https://www.bbraunusa.com/content/dam/b-braun/Ripple20

CISA (2020) Baxter ExactaMix (Update A). Available at https://us-cert.cisa.gov/ics/advisories/icsma-20-170-01

CISA (2020) GE Healthcare Imaging and Ultrasound Products. Available at https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

Dilibal Ç (2020) Development of Edge-IoMT Computing Architecture for Smart Healthcare Monitoring Platform. 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (SMSIT).

First.org (2021) Common Vulnerability Scoring System version 3.1: Specification Document. Available at https://www.first.org/cvss/specification-document

Haoyu L, Jianxing L, Arunkumar N et al. (2019) An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. Future Generation Computer Systems, 98 pp.69-77.

Jaidka H, Sharma N, Singh R (2020) Evolution of IoT to IIoT: Applications and Challenges. International Conference on Innovating Computing & Communications (ICICC) University of Delhi, 21-23 February Springer. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3603739

Kamani V (2020) A Detailed Guide to IoMT Implementation in 2020. Available at https://arkenea.com/blog/iomt/

Key factor (2021) State of Machine Identity Management Report 2021. Available at https://www.keyfactor.com/state-of-machine-identity-management-2021/

For full references, please email edito@healthmanagement.org or visit https://iii.hm/1isd

STERILE
Aquasonic
100
ULTRASOUND TRANSMISSION GEL
WATER SOLUBLE
LOT
PARKER
PARKER LABORATORIES, INC.
20 GRAMS
STERILE R
GUARANTEED STERILE UNLESS OPENED OR DAMAGED
CE 2797

HealthManagement.org

Promoting Management and Leadership