Mario J. Lorenzo

mario@mjlorenzo.com

Article Review of:

PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things

Yanambaka, V. P., Mohanty, S. P., Kougianos, E., & Puthal, D. (2019). Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things. *IEEE Transactions on Consumer Electronics*, *65*(3), 388-397.

Problem and Goal Addressed

Implanted Medical Devices (IMD) provide an effective means for monitoring the health of patients and enabling the practice of precision medicine that can yield a more informed diagnosis and optimized treatment for patients (Sun, Lo, & Lo, 2019). These devices can participate within a network fabric that can communicate with other implanted devices or with external controllers outside of the body. These external controllers can collect and transmit data between these devices and remote servers that process the data. These devices are collectively known as Internet of Medical Things (IoMT) devices. IoMT devices, like other IoT devices, are vulnerable to security attacks. One such vulnerability involves malicious devices eavesdropping or hijacking implanted devices with the intent to steal information or harm the patient (Rathore, Fu, Mohamed, Al-Ali, Du, Guizani, & Yu, 2018). The ability to authenticate devices within the IoMT fabric is an important aspect of security that helps mitigate many of these threats.

This article review examines a proposed authentication method for IoMT devices by Yanambaka, Mohanty, Kougianos, and Puthal (2019). They propose an authentication method called PMsec for IoMT devices that utilizes Physical Unclonable Function (PUF) module that can generate a unique key for each device and uses a two-phase enrollment and authentication process for authenticating devices within the IoMT network. Their work demonstrates that using a PUF module that is comprised of ring oscillators, multiplexers, and flip-flop, a device can generate a challenge-response pair that is unique to every device. The PMsec protocol uses a two-pass challenge-response system along with a stored hash that can be used to authenticate a device.

Prior Research and Significance

The emergence of Internet of Things (IoT) has led to a proliferation of small devices used to sense and control the environment such as a home or office building. This wave of innovation has similarly prompted great interest from the medical and scientific community seeking to instrument medical devices within the human body in order to collect information about organ function and control delivery of medications or provide therapy through the stimulation of nerves. The ability to implant small devices that can communicate with each other to sense and respond to biometric readings and trigger electromechanical, such as pace makers, or pharmacotherapy, such as insulin injection, or perform cardiac resynchronization therapy leading to artificial organs

that can coordinate with sensors and actuators across the body to perform complex organ functions. This area of research as led to a new field called Internet of Medical Things (IoMT) (Ivanov et al, 2018).

The need for improved security for IoMT is paramount as the popularity of these devices continues to grow. Some estimates project that IoMT devices will account for 30% of all IoT devices (Rathore et al, 2018). Currently only 2.3% of medical devices approved by the FDA include security features (Sun et al, 2019). With the rise of cyberattacks on the healthcare systems including profitable attacks such as randomware or selling of patient data on the dark-web, this poses a serious security threat.

Recent work in IoMT platforms have addressed various technical challenges when operating within an implanted medical device. These challenges include low-power consumption, limited processing power, battery life, and potential for tissue damage with using wireless mediums, such as WiFi and Bluetooth within the human body (Santagati & Melodia, 2017). These challenges and restrictions have opened a field of research to resolve many of these unresolved problems. Santagati et al (2017) propose an IoMT platform that uses Ultrasonic waves to safely communicate between implanted devices. They demonstrate the need for a device that must allow for a battery life of over 10 years. They also proposed a communication protocol that uses spreading codes and frequency hopping, allowing for multi-access channel with potential security for transmitted data between devices.

Other work by Rathore et al (2018) proposes a multi-layer security scheme for IoMT that generates a unique key by using an implanted echocardiogram (ECG) and uses Direct Sequence Spreading Spectrum (DSSS) to secure transmission between devices. Rathore et al (2018) and Santagati (2017) both use similar spreading code approaches for concealing transmission, however unlike Rathore et al (2018), Santagati et al 2017) does not make any direct claims about the level of security provided by their transmission approach.

Sun et al (2019), propose a best-practice as part of a survey for securing IoMT devices. Their work describes the various threats, including eavesdropping, replay attacks, man-in-the-middle, side channel leakage, and unauthorized access, as the primary threats to IoMT devices. Their work also explains why well-established cryptosystems such as public-key cryptography (RSA, Deffie-Hellman, DSA etc) are not suitable within IoMT environments due to the required computational power and the impact to the batter life of implanted devices that cannot be easily changed or recharged without a surgical procedure.

Methodology

Yanambaka et al (2019) propose an authentication scheme for IoMT devices called PMsec. PMsec calls for the inclusion of a PUF module to be placed within all IoMT devices. This includes implanted devices within or on the human body as well as edge servers that interact with these implanted devices. The PMsec module relies on a hybrid oscillator arbiter that is comprised of 256 oscillator rings, two multiplexers, and a flip-flop. Yanambaka et al (2019) assert that the manufacturing process of this physical component guarantees that each module is unpredictable, uncontrollable, and naturally random. As such, they make for an ideal key generator. The authors

also assert that because this key is built into the PUF module, no processing time is required to generate a key, as with conventional key generation algorithms. This avoids using processing time and reduces battery consumption on the device.

A PUF module takes as input what they call a “challenge” request in the form of a bit string and produces a “response” that generates a unique response. This means that no two PUF modules should produce the same response for a given challenge request.

The PMsec process involves two phases described as Enrollment and Authentication. The Enrollment phase is only performed once when a new IoMT device is introduced. This phase requires a two-pass challenge and response between the IoMT device and the edge-server (i.e. gateway) used to collect data. The process is like other chaining algorithms (like Cypher Block Chaining) where the Response produced by the device is used as the Challenge to the edge-server which in turn produces a Response that is used as a Challenge by the device. This process is repeated exactly two times and the final Response produced by the edge-server is then hashed and stored in a protected database. The authors point out that the database does not actually contain any of the challenge-response key pairs to avoid loss of integrity in the case that the edge-server were to be compromised.

During any future communications between the IoMT device and the edge-server, an authentication phase is used. The authentication phase is like the enrollment phase, where two passes of the Challenge-Response occurs between the PUF modules of the device and the edge server and the final response produced is then hashed and compared to the previously stored hash for that device-server enrollment. If the hash values match, the device is authenticated, otherwise, the device is considered malicious.

Because there can be errors during transmission of information between the IoMT device and the edge-server, the process is actually repeated up to 3 times in the case of a failed authentication to ensure that failed authentication was not due to a corrupted transmission of a challenge or response.

Further Research

Yanambaka et al (2019) performed theorical and practical experiments of the PMsec system. During their evaluation, they found that the average time to perform an authentication was 1.2 seconds to 1.5 seconds with an error rate of 10%. They assert that their work is first-of-a-kind for applying PUF to authentication in IoMT and therefore do not provide any comparisons against other systems. A brief search of the literature appears to support their assertion.

Their evaluation also concluded that the power consumption for interacting with the PUF module ranged between 121 to 285μW of power. They assert that this proves the use of the PUF was viable for real-world application. This is an important requirement for medical devices since availability and reliability requirements for the device to function properly for an extended period (over 10 years) is vital.

The work by Yanambaka et al (2019) does not address several open issues with security for IoMT devices. The work focuses on interactions between an IoMT device and an external edge-

server. Specifically, the authentication is only one-way authentication that authenticates the client but does not authenticate the server. This exposes a vulnerability where an adversary can place a malicious edge-server that challenges the various IoMT devices to enroll and subsequently steal information or interfere with the operation of the devices (such as an insulin pump). In order to protect against this kind of attack, the protocol should provide mutual authentication for both the client and the server.

The work by Yanambaka et al (2019) does not address the security of the transmission between the devices and the server. This means that an adversary can eavesdrop during the enrollment phase when a device is being added and store the challenge-response pairs. This can then be used as part of a replay attack to spoof or fool the IoMT device or the edge-server. One way to mitigate this issue is to leverage the work from Rathore et al (2018) and Santagati et al (2017) where they use various modulation techniques to conceal transmission of information using pseudo random spreading codes and frequency hopping.

Additionally, Yanambaka et al (2019) does not provide any authentication for devices that communicated directly in a peer-2-peer ad hoc network. These kinds of configurations allow for a medical sensor, such as a glucose reader, to communicate to an insulin pump located elsewhere on the body. The ability for these devices to authenticate each other exposes another kind of vulnerability.

The proposal by Yanambaka et al (2019) shows good progress in establishing authentication security model for IoMT devices, but additional work remains to arrive at a comprehensive security framework that protects against all known threats such as those outlined by Sun et al (2019) in their survey of IoMT security.

References

Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access*, *7*, 183339-183355.

Yanambaka, V. P., Mohanty, S. P., Kougianos, E., & Puthal, D. (2019). Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things. *IEEE Transactions on Consumer Electronics*, *65*(3), 388-397.

Ivanov, R., Nguyen, H., Weimer, J., Sokolsky, O., & Lee, I. (2018, May). OpenICE-lite: Towards a Connectivity Platform for the Internet of Medical Things. In *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)* (pp. 103-106). IEEE.

Rathore, H., Fu, C., Mohamed, A., Al-Ali, A., Du, X., Guizani, M., & Yu, Z. (2018). Multi-layer security scheme for implantable medical devices. *Neural Computing and Applications*, 1-14.

Santagati, G. E., & Melodia, T. (2017, May). An implantable low-power ultrasonic platform for the Internet of Medical Things. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications* (pp. 1-9). IEEE.