Contextual risk assessment for CIED medical devices.

This project is in collaboration with the JBZ hospital in 's-Hertogenbosch, the Netherlands.

Description of the research project

The security and safety of CIED devices cannot be accounted for separately. The programmability and monitoring functionalities of these devices represent a potential attack surface for a malicious attacker to exploit, resulting in potential threats to a patient's health. The effective security of these devices is "obscured" by the proprietary nature of the protocols and the software that they employ. Yet, several attacks affecting normal CIED (as well as other medical devices) operation have been showcased in the literature [1], and their potential impact to patient's health is documented [2,3].

However, these attacks are necessarily constrained by the contextual conditions in which they can be launched. For example, programming a CIED requires expensive equipment that is not readily available for anyone to buy on the market, and/or the attacker's physical proximity to the patient. Similarly, threats to the privacy of medical data transmission from "home base stations" are constrained by the necessity of performing man-in-the-middle attacks on the communication channel, or acquiring unauthorized access to the base-station. It is therefore an important goal to identify the contextual factors and conditions that need be satisfied for a specific attack to be successfully deployed.

This research project aims at identifying and measuring these factors through the study of real-world applications and deployment conditions in the JBZ hospital. This research builds on top of the Common Vulnerability Scoring System v3 (the world-wide standard for software and hardware vulnerability measurement) to extend its "Environmental" metrics to include considerations on vulnerability risk [4], in the same spirit of the recent MITRE-FDA joint effort in proposing metrics for the security of medical devices[1].

Candidate tasks

- Study the CVSS Environmental specification for vulnerability risk assessment in operative environments.
- Identify known CIED vulnerabilities and related attack procedure from existing documentation.
- Identify attack conditions related to the exploitation of the identified vulnerabilities.
- Perform *in-loco* technical assessments of attack conditions at the JBZ hospital in 's-Hertogenbosch.
- Evaluate risk on the basis of the CVSS environmental metrics.

[1] https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM419427.pdf

- Design and perform interviews with medical and technical personnel on employed (security) practices, precautions, training, perceived risk
- Design and perform interviews with hospital patients on security awareness, trust on technology
- Match the technical vulnerability and environment assessments with data from patients and practitioners to identify missing dimensions in the risk assessment.

Outcomes

This project's expected outcomes are:

- Technical and environmental assessment of CIED vulnerabilities in the JBZ 's-Hertogenbosch hospital following international standard guidelines
- Identification of guidelines for the improvement of CVSS metrics

If the candidate's work is well executed, this research results:

- Could be suitable for publication in a scientific venue (conferences and/or journals). This is a particularly important opportunity for candidates that intend to continue their scientific studies in a PhD programme.
- Could be discussed with the MITRE-FDA initiative for medical devices.

The study can be finalized in an "infographic" intended to communicate the research findings to the hospital's patients.

References

[1] Marin, E., Singelée, D., Garcia, F. D., Chothia, T., Willems, R., & Preneel, B. (2016, December). On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 226-236). ACM.
[2] SAMETINGER, Johannes, et al. Security challenges for medical devices. *Communications of the ACM*, 2015, 58.4: 74-82.
[3] Muddy Waters Capital LLC. http://d.muddywatersresearch.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf
[4] First.org CVSS Specification. https://www.first.org/cvss/specification-document