WiP Abstract: Methodology for Generating Attack Trees for Interoperable Medical Devices

Jian Xu
Worcester Polytechnic Institute
Worcester, MA, 01609
jxu3@wpi.edu

Vasiliki Syfrla
Unaffiliated
Grenoble,France
vasiliki.sfyrla@gmail.com

Krishna K. Venkatasubramanian
Worcester Polytechnic Institute
Worcester, MA, 01609
kven@wpi.edu

ABSTRACT

In this paper we present a methodology that provides a systematic way of generating attack trees for interoperable medical devices by leveraging process modeling, hazard descriptions, and fault-trees.

1. INTRODUCTION

Recent years have seen rapid growth in medical devices that can directly communicate with each other [1]. Such device systems are called *interoperable medical devices* (IMDs). IMDs are medical cyber-physical systems that enable effective patient care by coordinating patient-side medical devices in a clinically meaningful manner. IMDs have the potential to provide many clinical benefits such as a decrease in false alarms and real-time medication interaction checking [1]. Given the safety-critical nature of the IMDs, understanding the security threats that IMDs can be subjected to is essential. In the IMD context each threat essentially leads to patient safety issues, either in the short-term (e.g., untimely actuation) or long-term (e.g., loss of privacy leading to advanced persistent threats) .

2. ATTACK TREES IMD SECURITY

To understand the security issues with IMDs, we need to be able to model the threats in a meaningful manner and preferably quantify the level of security of the IMD under the threats— that is, determine the probability of the successful occurrence of the threat. In this regard, we present a methodology that helps systematically analyze IMDs for certain specific threats using the notion of *attack trees*. Once the attack trees have been developed, we can quantify their security conditions. An attack tree is a graphical model that contains a multi-level hierarchy of sub-trees, each representing a potential attack strategy, with the ultimate aim of reaching the root node, which is the goal of the attack and an undesirable event. In our previous work [2], we analyzed the security of an IMD performing patient-controlled analgesia (PCA-IMD), using attack trees. The idea was to look at a variety of ways that attackers can cause an over-infusion of pain medication into the patient's body. Though useful, this original approach was ad-hoc and consequently there was no way for us to evaluate if the trees covered a substantial portion of the attack surface leading to over-infusion.

ICCPS '15, Apr 14-16, 2015, Seattle, WA, USA

http://dx.doi.org/10.1145/2735960.2735993 ...$15.00.

We are consequently developing a more systematic methodology that, given a description of the workflow of a IMD and specific threats of interest, would generate an attack tree. Our methodology has three steps: **(1) Process Modeling:** In this phase, we use a process model tool to describe our IMD system. A process model is a description of the workflow of a process as it is executed in the real-world. The goals of a process model are to be able to keep track of what happens during a process. **(2) Fault-Tree Extraction:** Once the process model is built, it is converted into series of faults tree. A fault-tree is a top down deductive failure analysis in which an undesired state of a system is analyzed using Boolean-logic to combine a series of lower-level events. The fault-tree construction requires a hazard or undesired event that describes something that is not supposed to happen in an IMD system. Examples of hazards include: data from the electronic heath record (e.g., for sanity checking the expected infusion rate for the patient) is disrupted. The conversion process goes through the entire process model to determine which steps, if not executed correctly, lead to the hazard. For example an EHR disruption can be caused, among other ways, by loss of communication between the EHR and IMD setup. **(3) Attack Tree Generation:** Each fault tree generated in the last step indicates several attack paths to one specific hazard. The hazards can be thought of as a building block toward a 'high-level threats of interest" (e.g., over-infusion of pain medication in PCA-IMD). One can compose the hazards to create specific threat of interest. For example, EHR disruption in combination with disruption of device actuation can lead to over-infusion in specific conditions. The process of composing the individual hazards to form a high-level threat has the effect of combining the fault-trees to create an attack tree. Each leaf node within the fault-tree specifies a condition that if not satisfied leads to a hazard which then builds to a specific threat, and thus can be viewed as potential attacks on the system that eventually lead to the "high-level" threat.

3. FUTURE WORK

We are currently applying our technique to the PCA-IMD scenario to evaluate its effectiveness with respect to our earlier work. Our next steps are to quantify the security condition of the IMD with respect to a threat of over infusion.

4. REFERENCES

[1] D. Arney, S. Fischmeister, J. M. Goldman, I. Lee, and R. Trausmuth. Plug-and-play for medical devices: Experiences from a case study. *Biomedical Instrumentation & Technology*, 43(4):313–317, 2009.

[2] C. R. Taylor, K. Venkatasubramanian, and C. A. Shue. Understanding the security of interoperable medical devices using attack graphs. In *Proceedings of the 3rd international conference on High confidence networked systems*, pages 31–40. ACM, 2014.