An Analysis Method for Medical Device Security

Arnab Ray
Fraunhofer Center for Experimental Software Engineering
5825 University Research Court, Suite 1300
College Park, MD 2070
(240) 4872914
aray@fc-umd.edu

Rance Cleaveland
University of Maryland
Department of Computer Science
University of Maryland, College Park
MD 20740
7035857518
rance@cs.umd.edu

ABSTRACT
This paper is a proposal for a poster. In it we describe a medical device security approach that researchers at Fraunhofer used to analyze different kinds of medical devices for security vulnerabilities. These medical devices were provided to Fraunhofer by a medical device manufacturer whose name we cannot disclose due to non-disclosure agreements.

Categories and Subject Descriptors
D.4.6. Security and Protection (K.6.5)

General Terms
Security

Keywords
Medical Device Security

1. INTRODUCTION
The two primary drivers for the design of medical devices have historically been safety ("Is it possible for the device to harm the patient while operating in its intended environment?") and efficacy ("Will the device provide clinical benefit to the patient?") [1]. However a number of high-profile public demonstrations of successful attacks on devices and medical networks, has led to an increased public scrutiny on medical device security, prompting calls for security to be considered as another primary engineering driver for devices. In the past few years, several security researchers have shown that [2,3] that it is possible, through targeted attacks, to remotely gain control over an insulin pump and administer lethal doses to a patients, or to wirelessly induce fatal heart rhythms in a patient that uses a commercially available Implantable Cardioverter Defibrillator (ICD) [4]. In addition to custom attacks, devices have been subject to generic platform attacks like the Conficker worm [5] which targets any system running Windows, infected hundreds of MRI (Magnetic Resonance Imaging) devices in the world causing them to boot repeatedly.What is truly alarming about this statistics is the possibility that most of the successful attacks on medical devices would, by their very nature, never be reported or diagnosed as attacks.

HotSoS '14, Apr 08-09 2014,
Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04.
http://dx.doi.org/10.1145/2600176.2600192

As an outcome of the public concern expressed after the incidents referred to previously, the Government Accounting Office (GAO), in 2012, drafted a report that looked at medical device security particularly the FDA's role in ensuring that devices are analyzed for security (in addition to safety and efficacy)[6]. In 2013 the FDA published a preliminary guidance document [7] on device security for manufacturers. However there still exists apprehensions in the device community on how greater regulatory oversight on security and an increased threat profile would affect their engineering processes.

Designing for security is fundamentally different from designing only for safety and efficacy. Safety design decisions are based on the assumption that hazardous conditions (i.e. conditions which may harm the patient) occur accidentally, at random. An air-bubble enters the tubing because of improper connection to the reservoir, a power source blows out due to an anomalous surge, a wireless receiver accidentally picks up communication intended for another device. Increasingly though, we find that this random, accidental model of "bad environmental input" no longer holds true as attackers try to trigger hazards in devices through intentional, well-thought-out and often repeated attempts. As an example, an attacker, intent on denying medical services to a patient, would not only drain the battery through some mechanism but also deactivate the "low battery" alarm, in effect making independent failures (battery and the alarming software) have a common "cause". Thus most of the hazard-mitigation measures that exist in devices do not take into account malignant intent since they assume independent failure. The response of manufacturers has been to focus on post-facto ad-hoc approaches ("Let's put encryption on the communication") rather than on fundamental changes to the "science" of their engineering and assurance approaches.

In this poster, we will outline a structured methodology for analyzing a medical device for security vulnerabilities. The input to the methodology is the medical device and all associated software design artifacts (hazards analysis document, safety and functionality requirements, design specifications, communication protocol specifications etc)

2. METHODOLOGY

1. *Identify the hazards of interest to attacker*

In medical device design, engineers follow a risk-driven approach where they first identify the set of all hazardous conditions (anything that can harm a patient or care-giver) together with the risk of that hazard happening. Then they take a decision as to whether that hazard i) can be eliminated (i.e. a mechanism devised that makes the hazard impossible) ii) mitigated (i.e. detected and counter-measures taken so that no harm results from the hazard) or ii) absorbed in residual risk (usually done when the hazards cannot be eliminated or mitigated). One of the outputs of this hazards-analysis process is a table in which all the hazards are enumerated together with how each of them is handled. A good point from where to start the security-design process is this table. The intuition behind this is as follows. An attacker's primary aim would be to trigger one or more hazards, so that the patient ends up getting harmed. In this phase, our aim should be to identify all the hazards that may conceivably be triggered by an external agent with malignant intent.

2. *Identify attack surfaces*

In this phase, we identify all interfaces that the device provides to the outside world. Each such interface is a potential attack surface. Examples of possible attack surfaces: the keyboard through which user-input is taken, wireless communication between a controller and device, a network connection to another entity, an USB/Firewire/Bluetooth/IR connection that allows data and control information be exported or imported out of the device or one that allows software updates/patches to be applied.

3. *Enumerate attack scenarios*:

For each hazard H identified in Step 1 and each attack surface A identified in Step 2, we check to see if H can be triggered through A. If it is possible, we craft an attack scenario by which H would be triggered through A. The trick here is to create attack scenarios such that the mitigations put in place for the hazard H are bypassed. From the experience of the author, if the original mitigations were formulated without considering malignant intent as a hazard-cause, the devised mitigations are often not robust enough to deal with an intentionally triggered hazard. Work done by Halpern et al [4] contains different kinds of attack scenarios executed on an IED involving command injection, denial of service and reading unencrypted packets.

4. *Devise a measure for ranking attack scenarios*:

Once we have identified a set of attack scenarios, our next task should be to rank them in order of "importance". The intuition is again risk-management-driven---we will try to eliminate or mitigate the more important attack scenarios while perhaps absorbing the low-priority ones into residual risk. Any ranking scheme should take into account a few factors like how difficult is it for an attacker to execute the particular scenario (how far does he need to be from the patient, what kind of equipment he needs to possess, how much time would it take to execute the attack) and the reward the attacker gets (how much damage can he do to the patient or financial benefit can he derive) for a successful scenario execution.

5. *Devise counter-measure in a "safety and efficacy"-aware way*:

For every attack scenario, we need to define counter-measures (unless we decide to factor the vulnerability into residual risk). These counter-measures, depending on the attack scenario, could take different forms, be it additional hardware that "shields" the wireless communication to time-stamping of packets, encryption of data, mechanisms of role-based authentication and access-control. The point to consider is that none of these countermeasures should compromise patient safety. If encrypting traffic between a device and its controller consumes so many CPU cycles that it drains the battery very fast, and compromises the availability of treatment, that countermeasure should be rejected, perhaps in favor of a sub-optimal one, which would still be safe. If the use of password makes a device more secure, but entering the password requires a user to type a secure alphanumeric password every time he/she wants to operate the device using a small input device, the human-factors risk introduced by such a countermeasure (the device is so unusable that patients will reject it) would make it infeasible.

One vital factor to consider is that security measures may have to be bypassed in case of an emergency situation. For example, consider the following scenario. A device needs a password to operate. But the patient, who is the only one who knows the password, has become insensate. In such situations, caregivers need to be given emergency access to the device that side-steps the normal countermeasures. Needless to say, this is a challenging design requirement since an attacker would also attempt to exercise the security-overriding mechanism. This is also an area where safety considerations should override security, but such that the risk introduced by sub-optimal security countermeasures is less than the risk introduced by a measure that could delay treatment to a patient when it is urgently required.

3. REFERENCES

[1] FDA Guidance. http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/HomeHealthandConsumer/HomeUseDevices/ucm204884.htm

[2] Lethal medical device hack taken to next level. http://www.cso.com.au/article/404909/lethal_medical_device_hack_taken_next_level/

[3] Black hat hacker can remotely attack insulin pumps and kill people http://www.cbsnews.com/8301-501465_162-20088598-501465.htm.

[4] Halperin et al, Pacemakers and Implantable Cardiac Defibrillators:Software Radio Attacks and Zero- Power Defenses. IEEE Symposium on Security and Privacy. 2008

[5] Confickered! Medical Devices and Digital Medical Records Are Getting Hacked http://www.massdevice.com/blogs/massdevice/confic kered-medical-devices-and-digital-medical-records- are-getting-hacked

[6] FDA Should Expand Its Consideration of Information Security for Certain Types of Devices http://www.gao.gov/products/GAO-12-816

[7] Premarket Submissions for Management of Cybersecurity in Medical Devices. http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356186.htm