Emerging Frontiers in Embedded Security

Mehran Mozaffari Kermani†, Meng Zhang†, Anand Raghunathan‡, and Niraj K. Jha†
† Department of Electrical Engineering, Princeton University, Princeton, NJ 08544
‡ School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907
† ‡ † raghunathan@purdue.edu

Abstract—Computing platforms are expected to be deeply embedded within physical objects and people, creating an Internet of Things. These embedded computing platforms will enable a wide spectrum of applications, including implantable and wearable medical devices, smart homes, smart meters, brain-machine interfaces, physical infrastructure monitoring, and intelligent transportation systems. Unfortunately, the explosion in devices and connectivity creates a much larger attack surface, opening up new opportunities for malicious people and entities. Unless significant attention is paid to security, the Internet of Things could well be turned into an Internet of “Things to be Hacked”!

In this paper, we provide an overview of trends in embedded computing and highlight their implications on secure embedded system design. While embedded security is not a new topic, we argue that the characteristics and usage models of emerging embedded computing platforms necessitate a fresh look at embedded security and new approaches to secure embedded system design. We discuss the challenges using two case studies, viz., medical devices and smart homes. We provide examples of hypothetical and real security attacks, discuss the unique security challenges faced by these systems, and describe some initial efforts towards addressing them.

I. INTRODUCTION

Embedded computing platforms have been used in a range of application domains such as mobile appliances (phones, personal digital assistants, and multimedia players), smart cards, communications infrastructure, automotive, aviation, and industrial automation and control. As embedded systems increased in complexity, programmability, and network connectivity, information security emerged as a significant concern. The collective and individual security challenges of embedded systems in various application domains have been the subject of considerable research over the last two decades. Functional security mechanisms (cryptography, secure communication protocols, biometrics, anti-malware tools, intrusion detection, etc.), which were often originally developed in the context of general-purpose computing, can also be applied to embedded systems. However, unique challenges arise due to the processing, power, and assurance “gaps” [1], [2], necessitating security as a consideration during the design process rather than as an afterthought. The challenges that are commonly addressed in secure embedded system design research include efficient cryptography and security processing, and designing hardware and software that are resistant to various kinds of attacks. Efforts to address these challenges have led to (and will continue to lead to) several useful innovations.

However, the face of embedded computing is expected to change significantly in the near future, as computing systems are embedded more deeply and ubiquitously into the fabric of our lives. Some examples of emerging embedded applications are:

- Implantable and wearable medical devices (IWMDs) that diagnose, monitor, and treat a wide range of medical conditions or improve our lifestyles.
- Smart homes/buildings and spaces, which recognize occupants and improve their comfort and productivity, while simultaneously reducing their energy footprint.
- Implantable and wearable medical devices (IWMDs) that diagnose, monitor, and
- Smart grids for more efficient, reliable, and sustainable generation and delivery of energy.
- Brain-machine interfaces, which augment or replace traditional human-computer interfaces.
- Systems that monitor physical infrastructure to improve their safety and sustainability.
- Intelligent automobiles and transportation systems that improve the safety and efficiency of transportation.

These application trends warrant a fresh look at embedded system security, and the concomitant design challenges that it presents, for the following reasons:

- These systems are increasingly integrated into insecure physical environments – leading to greater exposure to attackers.
- The applications have unique usage models and, as a result, traditional security solutions may not be applicable or may not suffice. For example, medical implants may need to provide access to previously “unknown” entities such as emergency responders, precluding the use of encryption.
- The systems have transient usage patterns, where access privileges need to be defined over time and space, not just by the user.
- The number of embedded systems per human user will drastically increase – making it impractical for users to explicitly perform system administration tasks such as security patching, etc.
- Many of these systems will need to be transparently integrated into the environment and operate using energy scavenged from environmental sources – the consequent size and energy constraints imposed on any security solutions are extreme.

Acknowledgments: This work was supported by NSF under Grant no. CNS-0914787 and CNS-1219570.
Despite these new security challenges, the embedded systems of tomorrow will be relied upon to perform more and more safety and life-critical functions, making it essential to provide the right security solutions before successful attacks are launched (since the cost of being reactive will often be too high).

In this paper, we provide an overview of trends in embedded computing and highlight their implications on secure embedded system design. We utilize two concrete applications – medical devices and smart homes – to analyze the unique security challenges that are likely to be faced by emerging embedded applications.

IWMDs are used to diagnose, monitor, and treat a wide and increasing range of medical conditions. Successful security attacks on these systems can have severe consequences – ranging from loss of privacy to life-threatening situations. Unfortunately, the unique usage models and extreme resource constraints of IWMDs make the use of conventional security solutions like cryptography invalid or infeasible.

Smart homes are expected to provide increased convenience and comfort to their occupants, while improving energy efficiency [3], [4]. However, security and privacy threats can undermine these benefits and impede the adoption of smart home technologies. The large range and heterogeneity of devices, together with the wide range of users (with different levels of expertise in computing and information security), make this a challenging application from the security perspective.

We provide examples of hypothetical and real attacks for each of these application scenarios, and argue why traditional security solutions are insufficient. We also describe some initial efforts towards addressing security challenges and discuss important open problems.

II. IMPLANTABLE AND WEARABLE MEDICAL DEVICES

IWMDs are perhaps one of the most security-critical classes of embedded systems, because they frequently perform life-critical or health-critical functions. Examples of IWMDs, some of which are presented in Fig. 1, include implantable cardioverter defibrillators (ICDs), diabetes therapy systems, epileptic seizure detection and treatment systems, cochlear implants, heart rate monitors, and wrist oximeters. Most IWMDs are based on embedded microcontrollers that run software of significant complexity. Frequently, IWMDs also include wireless network interfaces that are used to communicate with external monitoring or diagnostic equipment, and to reprogram the device to optimize the delivered therapy. It is expected that future generations of IWMDs will be connected to form body area networks (BANs), e.g., using the recently-standardized IEEE 802.12.6 [5].

The increased functional complexity, software programmability, and network connectivity of IWMDs are desirable due to the resulting improvements in quality of monitoring and therapy, and patient convenience. However, they also increase security vulnerabilities and the risk of malicious attacks [6]. Unfortunately, the security of IWMDs has not received much attention until recently. Furthermore, securing IWMDs is not simply a matter of adding cryptography or secure communication protocols, for two major reasons.

First, IWMDs, in particular implantable devices, are subject to extreme resource constraints. For example, cardiac devices are often expected to run for over 10 years on a limited-size battery, since replacing the battery requires surgery. The limited battery capacity, in turn, places stringent limits on processor capability and memory size. This makes utilizing conventional security solutions close to impossible. It is well known that secure communication requires a combination of symmetric-key cryptography (to preserve confidentiality of the communicated data), message authentication (for integrity protection), and public-key cryptography (for peer authentication and key exchange) [7]. Public-key cryptography, in particular, presents significantly higher processing, memory, and energy requirements. Although the efficiency of public-key cryptography has been considerably enhanced over time, well-established public-key cryptosystems such as RSA, Diffie-Hellman, and elliptic curve cryptography (ECC) remain prohibitively expensive [8]. Recent developments in pairing-based cryptography are promising (the cost of pairings, the most expensive primitive in pairing-based cryptography, has been decreased to 1.90s on the ATmega128L microcontroller and 1.27s on the MSP430, and 0.14s on the PXA27x processor [9]). However, energy and code size are still significant concerns. Finally, key distribution for public-key cryptography is still a major hurdle.

The second reason why current IWMDs typically do not employ cryptographic measures is that they could impede emergency responders from communicating with the device in the event of a medical emergency. Any emergency responder or hospital serving a patient with an IWMD would need to have either a valid certificate (in the case of public-key based authentication) or the correct secret key (in the case of pre-shared symmetric key based authentication).

Due to the above challenges, current IWMDs rarely employ cryptographic protection for their wireless communications, implying that the wireless channel is quite susceptible to malicious attacks. Indeed, recent efforts have demonstrated successful attacks on cardiac pacemakers [10] and insulin pumps [11], [12].

Next, we analyze security issues in IWMDs through characterization of threats and associated risks.

A. Vulnerability Assessment

IWMD security shares the high-level objectives of traditional information security: confidentiality, integrity, availability, and privacy. However, the consequences of successful attacks can be much more severe than in many other classes of embedded systems.

We next present and categorize various hypothetical and real (demonstrated) security attacks on IWMDs.

1) Wireless attacks: Since cryptographic protection is often not employed by IWMDs for wireless communication, attackers can launch wireless attacks that disclose private data, provide incorrect inputs, and maliciously reconfigure the IWMDs. Such a reconfiguration could be performed with the intention of harming the patient by failing to deliver treatment when necessary or by delivering treatment when unnecessary.
A successful wireless attack on an ICD is demonstrated in [10]. The research shows how the ICD’s design, which involves wireless communication with an external programmer, can be exploited by an attacker. By reverse-engineering the communication protocol, the attacker can launch wireless attacks, with consequences ranging from disclosure of private data (compromising confidentiality) to alteration of device settings (compromising integrity). In the worst case, the attacker can maliciously reconfigure the ICD to harm a patient by inaction (failure to deliver treatment when necessary) or by delivering a electrical stimulus when the heart is beating normally.

Using a similar approach, the study in [11] implements a successful attack on a glucose monitoring and insulin delivery system, exploiting both the wireless channel between the device and external controller, and the wireless channel between devices. The attacker first eavesdrops on the wireless packets sent from a remote control to an insulin pump, and reverse-engineers the communication protocol. The same eavesdropping attack is performed on a glucose meter that sends the glucose-level data to the insulin pump. The attacker also discovers the PINs associated with the remote control and glucose meter. By mimicking the remote control, the attacker can configure the insulin pump to disable or change the intended therapy, stop the insulin injection, or inject a much higher dose than necessary. By mimicking the glucose meter, the attacker can send incorrect glucose-level data to the insulin pump, causing the pump to adjust insulin delivery based on the false data. Later efforts built on this attack to increase the range of the attacker and further automate the attack process [12], [13].

With the knowledge of the communication protocol, denial-of-service attacks that aim to drain an IWMD’s battery power may be launched through the wireless channel. If the IWMD responds to each incoming communication request from attackers, its battery may simply die soon and need to be surgically replaced. An attacker could also generate a large amount of noise to jam normal communication if he simply knows the approximate frequency of transmissions. In either case, on-time therapy delivery (availability) could be compromised.

2) Malware and vulnerability exploits: Various forms of malware, including viruses, worms, Trojans, keyloggers, botnets, and rootkits, have affected general-purpose computing platforms. Smartphone platforms, such as Symbian and Android, have already been breached by mobile malware [14]. With the increasing flexibility and connectivity of IWMD platforms, it is just a matter of time before they are adapted to target IWMDs.

For example, Intel Health Guide [15] is a chronic care product that delivers personalized health monitoring at home. Patients can use the system to measure their own vital signs and, through the Internet, upload the results to a remote server, where healthcare professionals can assess the patient’s health condition. A virus that infects such a system can examine, delete or forge health data, and thus compromise data confidentiality and integrity.

Furthermore, since software is often highly complex and difficult to verify to be correct under normal inputs, let alone malicious inputs, software vulnerabilities are inevitable and difficult to detect. A common example of software vulnerabilities is a buffer overflow, wherein software is manipulated to write past the bounds of a memory region, potentially overwriting the address to an instruction, to which the program is later redirected. If a buffer overflow is triggered by especially-crafted user inputs, causing the redirected program to execute malicious code, it is called a buffer overflow attack. With even limited knowledge of the software running on IWMDs, attackers can exploit buffer overflow vulnerabilities, as well as other software vulnerabilities, to cause the devices to reveal private information or change device settings.

3) Side-channel attacks: Employing statistical analysis of side-channel information leaked through physical channels (implementations), such as power consumption and execution time, side-channel attacks infer sensitive information [16]–[18]. These attacks can potentially be mounted against IWMDs. For example, suppose communications between implanted pacemakers and external programmers are encrypted, and the same secret key is shared by all pacemakers of the same model so that the emergency responders can access the device in case of an emergency. If an attacker has access to a pacemaker unit, the secret key can become a vulnerable target for differential power analysis [16], a form of side-channel attack that utilizes power consumption information. Once successful, the attacker could reveal and publicize the secret key and thus make the cryptographic protection ineffective.

Examples of several IWMDs and their associated security...
In Table I, Column 1 corresponds to IWMDs. Column 1 lists the types of attacks they are prone to. Column 2 enumerates the security risks associated with each system with respect to a particular attack. Confidentiality, integrity, availability, and privacy risks are abbreviated as C, I, A, and P, respectively.

### B. Possible Countermeasures

In this section, we discuss possible defense solutions and their advantages and drawbacks.

1) **Close-range communication:** Limiting the communication range (between IWMDs and external controllers), using near-field communication (NFC) [19] or RFID, is effective in limiting wireless attacks [20]. Nonetheless, attackers with high-gain antennas can still attack the wireless channel. For example, the attacker can access the IWMD wireless channel from up to ten meters away in the case of RFID [21], [22] and one meter in the case of NFC [19].

An alternative is body-coupled communication that uses the human body as the transmission medium in which the communication range is limited to the proximity of the human body [23]. However, even such close-range communication schemes cannot defend against all close-range attacks (which, for example, may be feasible in a crowded place).

In addition to communications that are designed to be inherently short-range, measures can be taken to enforce close-range communication. An access control scheme based on ultrasonic distance-bounding is introduced in [24], in which an IWMD grants access to its resources to only those devices that are close enough. Physical shielding is another way of enforcing close-range communication. A metal shield that restrains wireless signals from traveling beyond it can effectively eliminate radio eavesdropping from attackers at a distance.

2) **Cryptography:** As mentioned before, conventional cryptographic methods are not directly applicable to deeply embedded IWMDs because of their resource constraints as well as the problem of distributing keys to legitimate parties. One possible solution to the key distribution problem is to ask patients to carry cards or bracelets imprinted with the secret keys of their IWMDs. The keys could be printed into the patient’s skin using ultraviolet-ink micropigmentation [25] that only becomes visible under ultraviolet light.

IMD Guardian [26] presents a cryptographic scheme for implantable cardiac devices in which no pre-distributed secrets are required, and the patient’s electrocardiography signals are used for key extraction, similar to the use of other biometrics for key generation. The major concern with this approach is the robustness and reliability of the keys extracted from physiological characteristics. Furthermore, it might still be possible to steal the key through physical contact with the patient.

3) **External devices:** To preserve IWMD battery power, the verification of its incoming requests can be offloaded to a trusted external device. One such device is the Communication Cloaker [27]. It mediates communications between the IWMD and pre-authorized parties, and enables the IWMD to ignore incoming communications from all unauthorized programmers.

Another external device is a personal base station called the “Shield” [28]. It works as a relay between the IWMD and external programmer. It is designed to receive and jam the IWMD messages at the same time, so that other radios cannot decode them. It then encrypts the IWMD message and sends it to the legitimate programmer. This solution requires changes to external programmers, but no changes are required to IWMDs; therefore, it may be applied to already deployed systems.

4) **Secure execution environment:** Due to the relative ease and low cost of launching software attacks, which could subvert the medical software that executes on IWMDs, including the operating system, it becomes essential to provide a secure execution environment for the security-critical medical software in the face of other untrusted applications and also an untrusted operating system. The isolation may be based on physical separation (e.g., IBM’s secure co-processor [29]) or logical separation, in which both the sensitive and untrusted code are run on the same processor, but are isolated either using an additional layer of software, such as virtualization, or additional hardware support (e.g., Intel TXT [30] and ARM TrustZone [31]).

Trusted computing [32] constitutes a set of standards such as the trusted platform module (TPM). It is gaining wide popularity in general-purpose computing systems. In size- and resource-constrained platforms, it is currently not common to see hardware TPMs. In such cases, a software TPM based on software emulation of TPM functions within an isolated execution environment could be used [33].

Table II summarizes the above-mentioned solutions along with the specific types of threats that each solution can defend against. Column 1 refers to the defense techniques. Column 2 corresponds to the threat that each solution can defend against. Columns 3-6 provide the security evaluation for each defense solution against the corresponding threat.

### III. Smart Homes

Homes are becoming smart through the introduction of various deeply embedded devices that act autonomously. To date, various research prototypes of smart homes have been developed, e.g., MIT’s House_n [3] and Georgia Tech’s Aware

---

### TABLE I

<table>
<thead>
<tr>
<th>System/Device</th>
<th>Threat</th>
<th>C, I, A, P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacemaker and ICD</td>
<td>side-channel attack</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Insulin pump</td>
<td>side-channel attack</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Deep brain stimulation system</td>
<td>side-channel attack</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Intrathecal drug delivery</td>
<td>side-channel attack</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Fall detector</td>
<td>wireless attack</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Health Guide</td>
<td>malware and vulnerability exploit</td>
<td>C, I, A, P</td>
</tr>
<tr>
<td>Heart rate monitor</td>
<td>wireless attack</td>
<td>C, I, A, P</td>
</tr>
</tbody>
</table>
homes a potentially ripe target for security attacks. That users have widely varying levels of expertise, make smart administrators (with overlapping access control), and the fact communication standards and protocols), sensitive and confidential appliances inside smart homes (that use heterogeneous communication, NFC, BCC, access control based on distance Cryptography “Cloaker” “Shield” Secure execution environment

Table II: Security Evaluation of Defense Solutions

<table>
<thead>
<tr>
<th>Defense</th>
<th>Threat</th>
<th>C</th>
<th>I</th>
<th>A</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID-based communication, NFC, BCC</td>
<td>long-range wireless attack</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Cryptography</td>
<td>wireless attack</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>“Cloaker”</td>
<td>wireless attack</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>“Shield”</td>
<td>wireless attack</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Secure execution environment</td>
<td>malware and vulnerability exploit</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Fig. 2: Structure of a typical smart home (modified and adopted from [40]).

A typical smart home, shown in Fig. 2, may consist of deeply embedded sensors, detectors, and control systems that are capable of gathering information and acting on commands received from the home occupants. These sensors and control systems could improve the comfort and energy efficiency of the smart home by regulating lighting, humidity, heating, ventilation, and air-conditioning (HVAC), make the home safer through surveillance, or integrate computing into entertainment systems and other home appliances.

Devices and appliances in a smart home communicate with each other through a communication network commonly referred to as the home area network (HAN). A wired networking technique commonly adopted in HANs leverages electrical outlets in the smart home to directly transmit data over conductors used for electric power transmission. This is denoted as PLC (Power Line Communication/Carrier) technology, e.g., the X-10 protocol [34] and INSTEON [35]. HANs may also use general wireless standards, such as Bluetooth [36], Wi-Fi [37] or NFC, as well as low-cost and low-bandwidth protocols specified for BANs, such as ZigBee [38] or Z-Wave [39].

A. Security and Privacy Concerns

Wireless interactions among a large number of devices and appliances inside smart homes (that use heterogeneous communication standards and protocols), sensitive and confidential nature of the information transmitted, presence of multiple administrators (with overlapping access control), and the fact that users have widely varying levels of expertise, make smart homes a potentially ripe target for security attacks.

Information transmitting nodes in smart homes, e.g., temperature, smoke, and humidity sensors, motion and window vibration detectors, are vulnerable to eavesdropping, which may reveal sensitive information about the occupants. In general, information leakage from humidity, temperature, or smoke sensors from the smart home may not be as important as information leakage on the motion and activity of occupants through surveillance systems, sensors integrated into windows or fingerprint readers.

Even if eavesdropping attacks are prevented, the privacy of the information collected legitimately is often still a concern. For example, it is projected that by the end of 2012, the number of smart meters in the U.S. will rise to more than 50 million. Although such meters offer various benefits, such as reduced greenhouse gas emissions and energy bills, they can potentially compromise privacy of home occupants by revealing usage trends of specific appliances to the utility company.

Controllable devices in smart homes receive commands from users or other devices to perform actions that impact the physical world. Attacks on these devices may therefore have physical consequences. For instance, an attacker may increase or decrease the temperature or humidity of the smart home by sending commands to the HVAC system. Although the severity of this attack is not high, the attacker’s intention may simply be to increase the utility bills or harm the health of the occupants. The attacker may also turn off the smoke detectors and surveillance systems, in order to suppress the monitoring capabilities of the smart home, for later misuse.

B. Open Problems

The unique nature of smart homes calls for revisiting and rethinking security solutions that have been applied in other contexts. As mentioned earlier, the major challenges posed by smart homes include dealing with a large number of devices, having to deal with many users with different levels of expertise, and allowing mixed ownership and access control.

1) Access control models: The usage models of smart homes may require new spatial and temporal access control models to be developed. For example, a user can be constrained to be physically present in the smart home (or in a particular room of the smart home) to get access to sensitive data or be able to control a device. Similarly, temporal access control can be adopted in smart homes, where access is limited to a specified time interval. However, the complexity of smart homes (both in terms of devices and users) makes scaling of existing access control mechanisms extremely difficult. Visitors, guests, temporary servicemen, and even the occupants of the smart home need different levels of access privileges. No existing solution adequately addresses the unique set of challenges posed by smart homes [41]. Moreover, the lack
of user experience (or different levels of expertise) creates problems in access control administration in smart homes.

2) Inexperience of home occupants: Obviously, the occupants of a smart phone cannot be expected to exhibit a level of expertise comparable to that of an experienced computer administrator. Inexperienced occupants, e.g., children or elderly, may unintentionally disclose confidential and sensitive information. Such an occupant may also reveal privacy-related information to potential adversaries, e.g., side-channel information about usage trends, time/history of usage, and operation logs. Therefore, simple-to-use interfaces to security solutions are critical.

3) Effort involved in software patches or updates: The sheer number and diversity of devices and appliances in smart homes make it difficult to provide them with updated security countermeasures. For instance, unlike a centralized information technology system, which is able to update software security patches through the network, differences in smart home devices make such automation difficult.

IV. CONCLUSIONS

New applications and usage models for embedded computing lead to new security challenges. In this paper, we discussed the emerging frontiers in security. Through two case studies, i.e., medical devices and smart homes, we elaborated upon the unique security challenges facing them. We believe that there is a strong need for research on addressing the security challenges of emerging classes of deeply embedded systems.

REFERENCES


[38] “ZigBee,” http://standards.ieee.org/.

