New Security Threats Related to IoT Nodes and Mobile Applications
extracted from deliverable D2.3

Lionel Morel, Damien Courousse (CEA),
Alberto Battistello, Eric Poiret, Victor Servant (IDEMIA),
Armand Castillejo, Olivier Caffin (ST)
Gudrun Neumann (SGS TÜV), David Hely (LCIS),
Philippe Genestier (Orange)
Healthcare is facing one of its major turning points in decades. Connected healthcare offers a way and will be an effective tool to address the needed reorganization of our health system. After penetrating the consumer market, the digital revolution and its related IoT (Internet of Things) concept is rapidly changing health models.

The Internet of Medical Things (IoMT) was born.

Analysts ‘Yole Development’ estimate that today there are more than 45 million IoMT devices and that the market will offer more than 235 million in 2020.

---

The Internet of Medical Things (IoMT) in the IoT world

(Source: Connected Medical Devices Market and Business Models 2017 report, Yole Développement, September 2017)
Attacks On Medical Devices

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

Date Issued: July 31, 2015

Cyberattacks on Medical Devices

Manufacturers designing medical devices need to be aware of vulnerabilities in their hardware and software.

Hacking, St. Jude Medical

FDA Safety Communication

Date Issued: January 9, 2015

Johnson & Johnson says insulin pump 'could be hacked'

4 October 2016 | Business

Security of IoMT: where are we?

Connected medical devices imply:
- New attack vectors appear
- **Attack surface** is much wider
- Need to ensure *end-to-end security*

EU regulations have appeared:
- IEC 62351-10, section 6
- GDPR

Need to follow these regulations:
*Technical innovation to deal with new security threats and risks.*
SERENE-IoT addresses the needs of patients remotely followed by professional caregivers by developing advanced smart e-health IoT devices and architecture in Europe.

- The core values of the project are:
  - High healthcare quality services
  - High level of trust (Security, Safety, Privacy, Robustness)
  - Efficient execution of requested operations and tasks
  - Interoperable and compatible systems
  - Solutions at much lower cost than the traditional care currently provided
SERENE-IoT will develop 3 medical clinical prototypes addressing 3 medical challenge domains:

**Domain 1: Remote Healthcare**
Moving care services from hospital to home.

First Low-power Medical IoT Module validated with 2 class IIx medical devices.

**Domain 2: Early detection**
Of Methicillin-resistant bacteria.

First Low-power Mobile Detector for MRSA i.e. antibiotic resistant bacteria.

**Domain 3: Fall Prevention/Detection**
Fully wireless insole for Fall Detection + Risk Monitor.

For each medical devices, SERENE-IoT will provide:

- **Evaluated Clinical Prototypes**
- **Multi-centric Clinical Investigation Plans**
- **IoT System Evaluation**
Context – IoT Medical Applications
A Tentative Generic IoMT Architecture

Connected Medical Devices

Gateway

Cloud Data Center

Applicative End-Point

Data Operator / User

Provider-controlled enclave

Need: end-to-end security
Security of the IoMT Chain

This presentation will focus on security for:

- The IoMT nodes
- The mobile application

We focus on Side-Channel Attacks in the sense of Spreitzer2018:

"**Side-channel attacks** do not exploit specific software vulnerabilities of the OS or any specific library, but instead **exploit available information** that either **leaks unintentionally** or that is [...]**published for benign reasons** in order to **infer sensitive information indirectly**."
Security of the IoMT Chain

**Local:** the attacker has a **physical access** to the HW platform, can observe some physical phenomena.

**Vicinity:** **eavesdrop** target's communication channels.

**Remote:** attacker only relies on **execution of code** on the target.
Security of the IoMT Chain

Passive: only observe leaking information

Active: influence behavior of target

- Power Analysis
- Net Traffic Analysis
- Wi-Fi signal mon.
- Data Usage Stats
- EM/Laser Fault Injection
- Cache-attacks
- Row-hammer
Security of the IoMT Chain

**Logical**: exploit **software** property

- Cache-attacks
- Row-hammer
- Net Traffic Analysis
- Data Usage Stats

**Physical**: exploit **hardware** property

- Power Analysis
- EM/Laser Fault Injection
- Wi-Fi signal mon.
Security of IoMT Devices

Assets

• Data (patient, institution, provider)
• Device firmware and configuration

(Security) Risks

• Data theft
• IP theft
• Denial-of-Service

Existing Counter-Measures

• HW: secure elements, shielding
• SW: masking, hiding, obfuscation,
Security of Mobile Applications

SERENE-IoT

Mobile Device

Software Stack

Hardware Platform

Patient Medical Conditions

Medical Device Status

Infrastructure

Install

Remove

Upgrade
Local Attacks on Mobile Platforms

Demonstrated, accessible attacks:

- **Electro-Magnetic Analysis** to retrieve AES key [Genkin 2016]
- **Power Glitching** to create SW faults [NewAE 2016, O’Flynn 2016]
- **EMFI** to skip instructions [Riviere 2015, Ordas 2017]
- **NAND Mirroring** to hard reset and brute-force passwords [Skorobogatov 2015]

Hard or not-demonstrated attacks:

- **Power-Analysis Attacks**
- **Clock Glitching**
- **Laser Attacks**
Vicinity Attacks on Mobile Platforms

- **Network Analysis** to fingerprint applications [Conti 2016a, Stöber 2013]

- **USB power analysis** to infer identity or visited websites. [Yang 2017, Conti 2016b]

- **WiFi signal** monitoring to detect screen patterns, eg unlock patterns via a notebook connected to the same « hotspot » [Ali 2015, Zhang 2016, Li 2016]

- **Network traffic alteration** to increase performance of website fingerprinting [He 2014]
Remote Attacks on Mobile Platforms

- Take advantage of **Linux-inherited procfs leaks** to:
  - Observe application’s **memory footprint** and infer browsing behaviors, application transitions [Jana 2012, Chen 2014]
  - Observe app’s **context switches** and infer finger movements [Simon 2016, Diao 2016]

- Observe and force system’s **page deduplication** to fingerprint visited website.

- **Micro-architectural (cache) attacks** measure cache access times to infer encryption keys, finger movement, etc. [Ge 2016, Szefer 2016]

- **RowHammer**: well-chosen memory writes change state of adjacent « logically protected » cells [VanDerVeen 2015, Kim 2014, Seaborn 2015, Gruss 2016]

- **Differential Computation Analysis**: observe memory accesses of White-box protected Crypto functions to deduce encryption key [Bos2016]

- And of course … **Reverse-engineering**
Security of Mobile Applications

Fault Attack

Mobile Device

SCA/DCA

SERENE-IoT (Assets)

Algebraic attacks

Key Extraction

Software Stack

Code Lifting

Hardware Platform
Security of Mobile Applications

Protection
(whitebox, obfuscation, polymorphism)

 Fault Attack
Mobile Device

Key Extraction

SCA/DCA

Algebraic attacks

Code Lifting

App

App

App

App

SERENE-IoT
(Assets)

Software Stack

Hardware Platform
SERENE-IoT: Expected Contributions

Security Requirements and Best Practices

- [SGS-TÜV] Compare existing security requirements with new threats and propose best practices for IoMT Security (Risk Analysis and Evaluation, Requirements, Threats <-> Countermeasures)

HW-level Security

- [LCIS] IoMT-device extensions against memory corruptions and hw attacks
- [STMicro] Develop and validate new μ-controller for sensitive firmware isolation

SW-level Security

- [IDEMIA] White-box cryptography
- [CEA] Combine code polymorphism with program encryption
- [Orange] Blockchain to implement consent management
Conclusion

- IoT is reaching medical devices and applications

- The use of open platforms (smartphone) introduces new risks:
  - Device is used in un-controlled environment
  - Unknown applications are executed concurrently on the same platform
  - Many attack vectors

- We need to guarantee **end-to-end security by-design**

- SERENE-IoT partners study:
  - HW protections against physical attacks
  - SW protections against attacks on mobile applications
  - Use of Blockchain to implement consent management


• [Conti 2016b] M. Conti, M. Nati, E. Rotundo, and R. Spolaor, Mind the plug! Laptop-user recognition through power consumption, in Proc. Workshop IoT Privacy Trust Security (IoTPTS@AsiaCCS), X’ian, China, 2016, pp. 37–44.


Selected Bibliography


