SERENE-IoT

Secured & **E**ne**R**gy **E**fficie**N**t h**E**alth**-**care solutions for **IoT** market

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)

June 2018

SERENE-IoT project is a project labelled within the framework of PENTA, the EUREKA cluster for Application and Technology Research in Europe on NanoElectronics

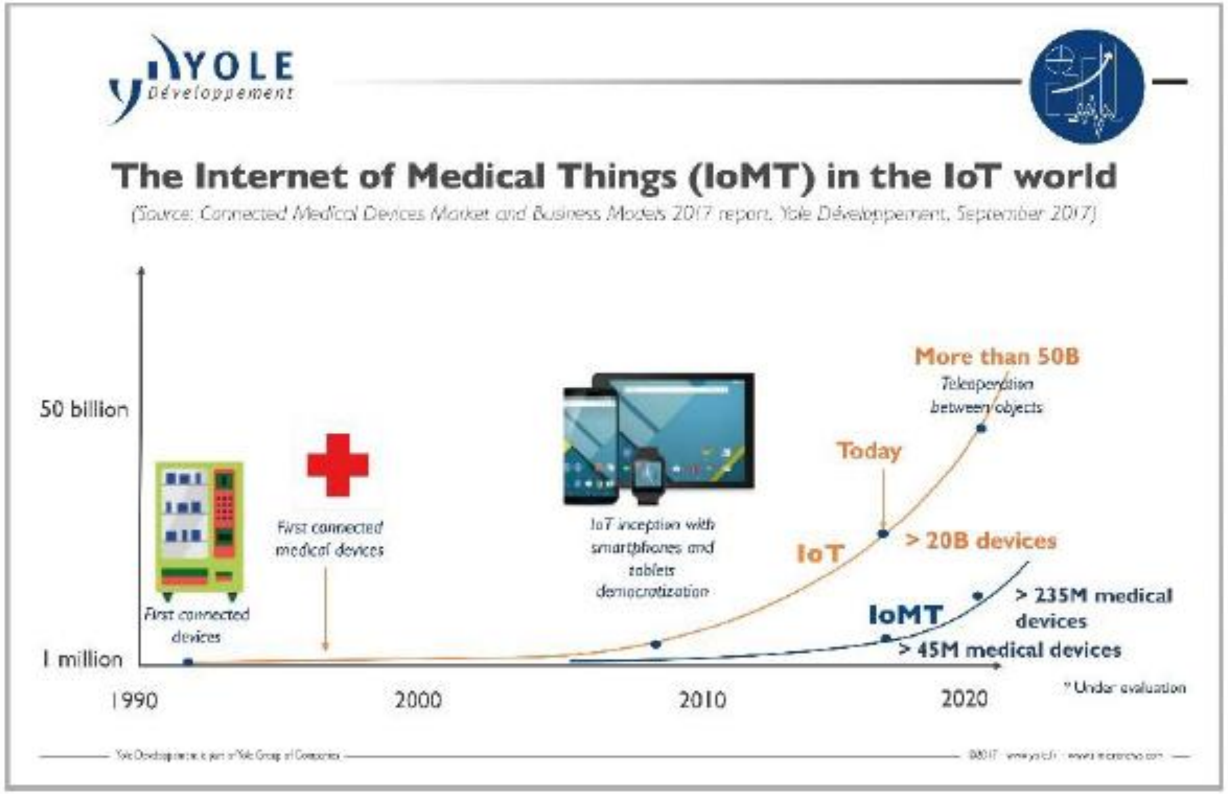
Connected Healthcare

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.

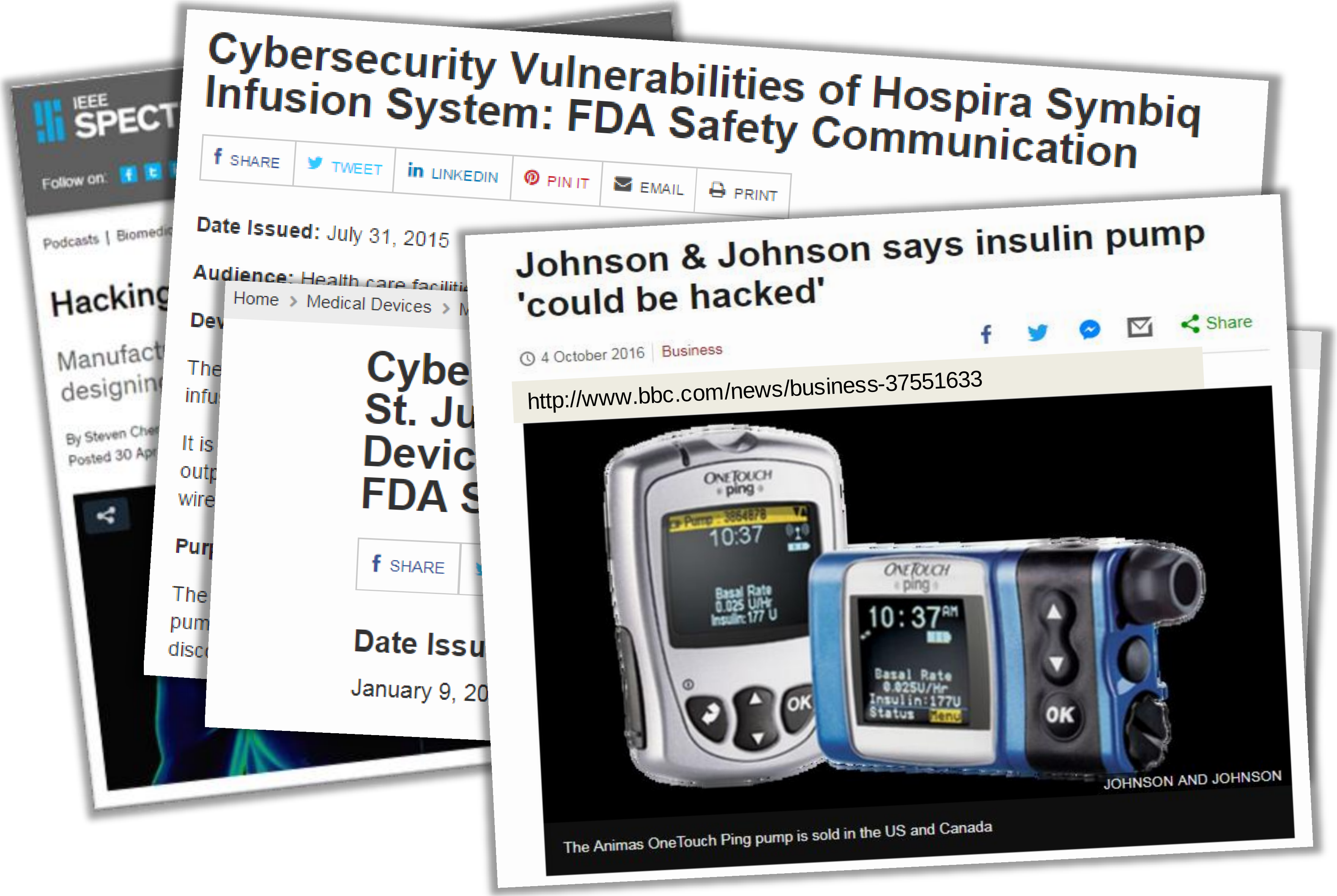
Analysts 'Yole Development' estimate that today there are more than 45 million IoMT devices and that the market will offer more than 235 million in 2020



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



IEEE SPECT

Follow on:

Podcasts | Biomedic

Hacking

Manufact
designin

By Steven Che
Posted 30 Apr

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

SHARE TWEET LINKEDIN PIN IT EMAIL PRINT

Date Issued: July 31, 2015

Audience: Health care faciliti

Home > Medical Devices > M

Cybe
St. Ju
Devic
FDA S

SHARE

Date Issu

January 9, 20

Johnson & Johnson says insulin pump 'could be hacked'

4 October 2016 | Business

Share

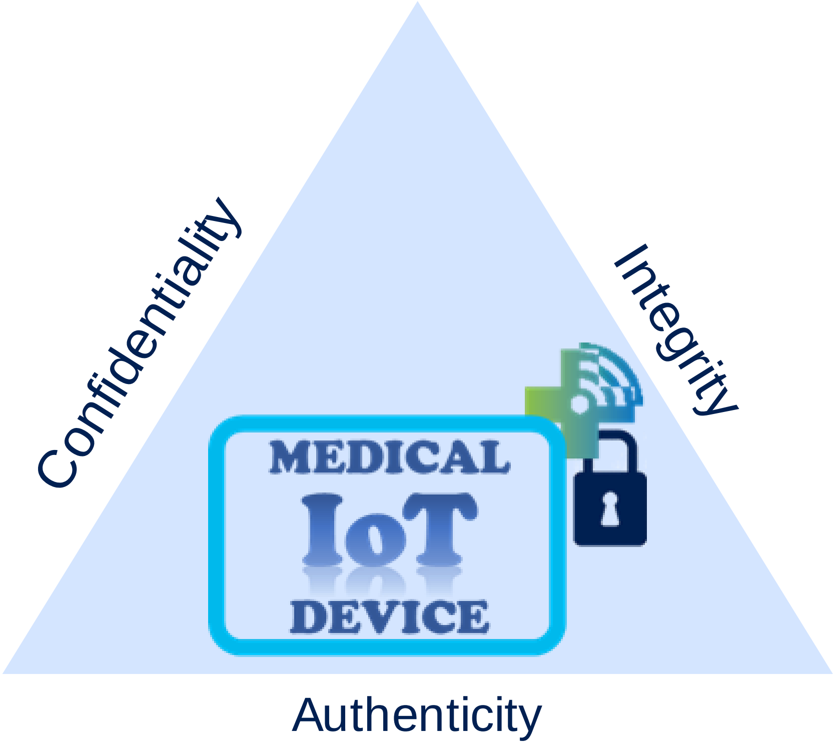
http://www.bbc.com/news/business-37551633

ONETOUCH ping
10:37
Basal Rate 0.025 U/Hr Insulin: 177 U
ONETOUCH ping
10:37 AM
Basal Rate 0.025U/Hr Insulin:177U Status Menu
OK
JOHNSON AND JOHNSON

The Animas OneTouch Ping pump is sold in the US and Canada

Originally from “Cybersécurité des dispositifs médicaux”, by Florian Pebay Peyroula, CEA, Medi’Nov 2018

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.

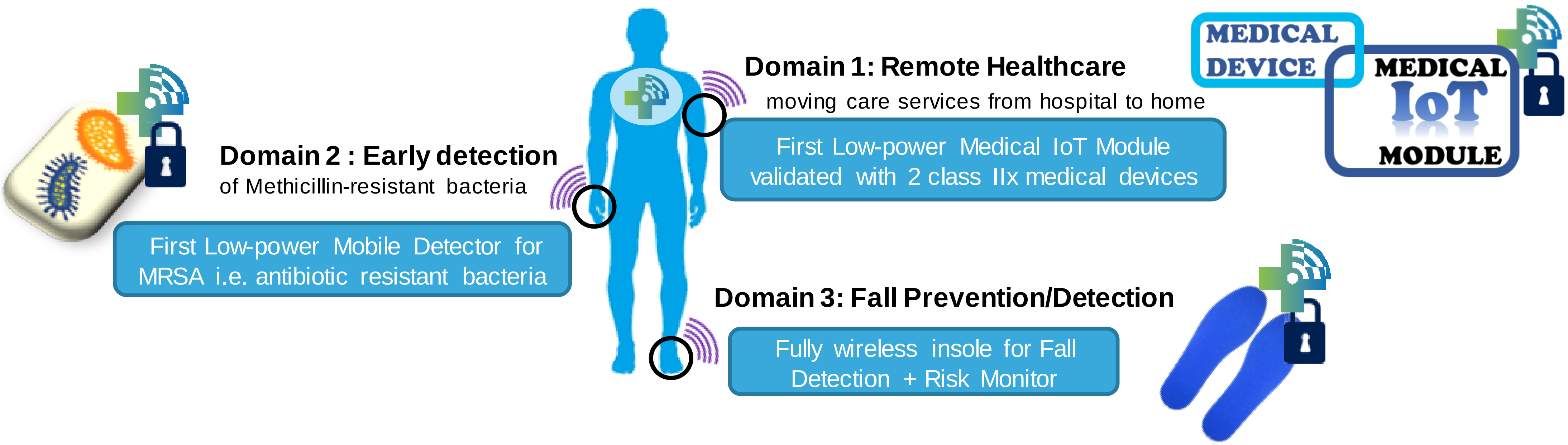
SERENE-IoT: Project Goal

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 : Outcomes

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

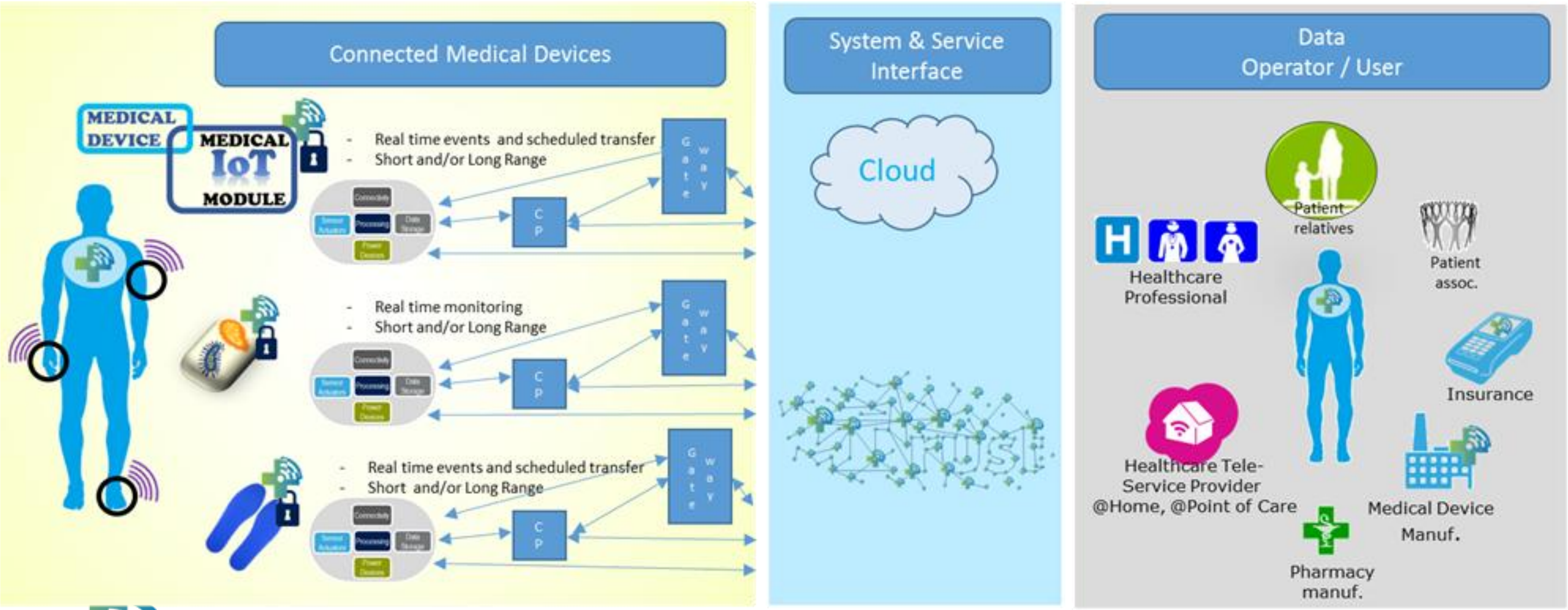
Domain 3: Fall Prevention/Detection

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



Connected Medical Devices

System & Service Interface

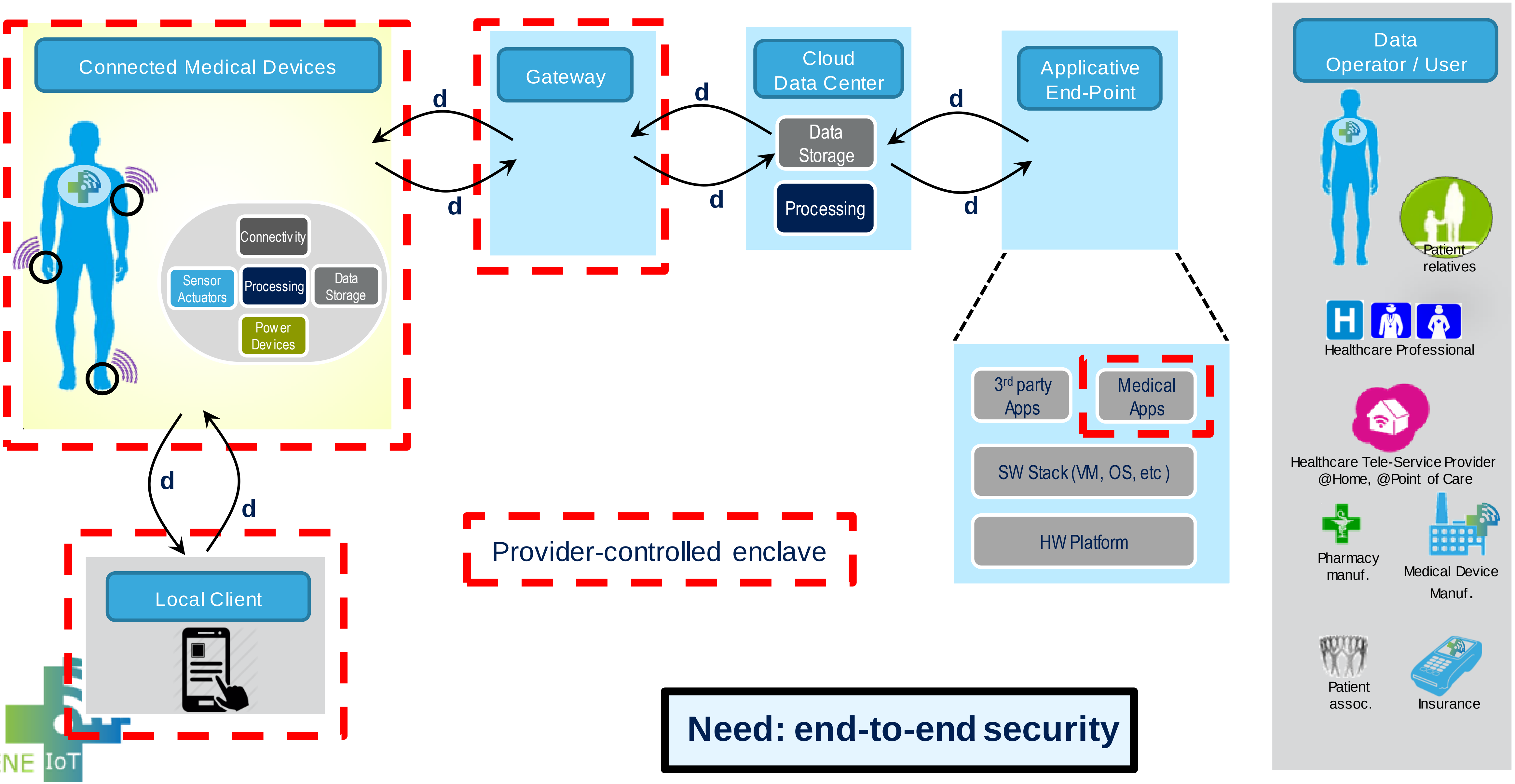
Data Operator / User

- Real time events and scheduled transfer
- Short and/or Long Range

- Real time monitoring
- Short and/or Long Range

- Real time events and scheduled transfer
- Short and/or Long Range

A Tentative Generic IoMT Architecture



Need: end-to-end security

Security of the IoMT Chain

This presentation will focus on security for:

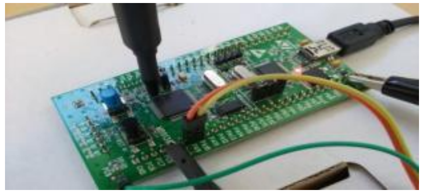
- The IoMT nodes
- The mobile application

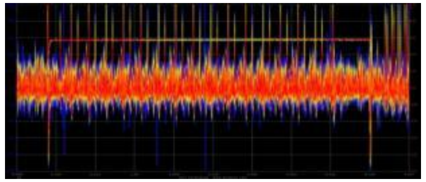
We focus on Side-Channel Attacks in the sense of Spreitzer2018:

*“**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**.”*

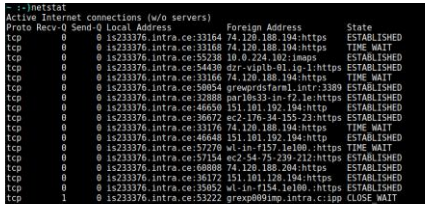
Security of the IoMT Chain

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

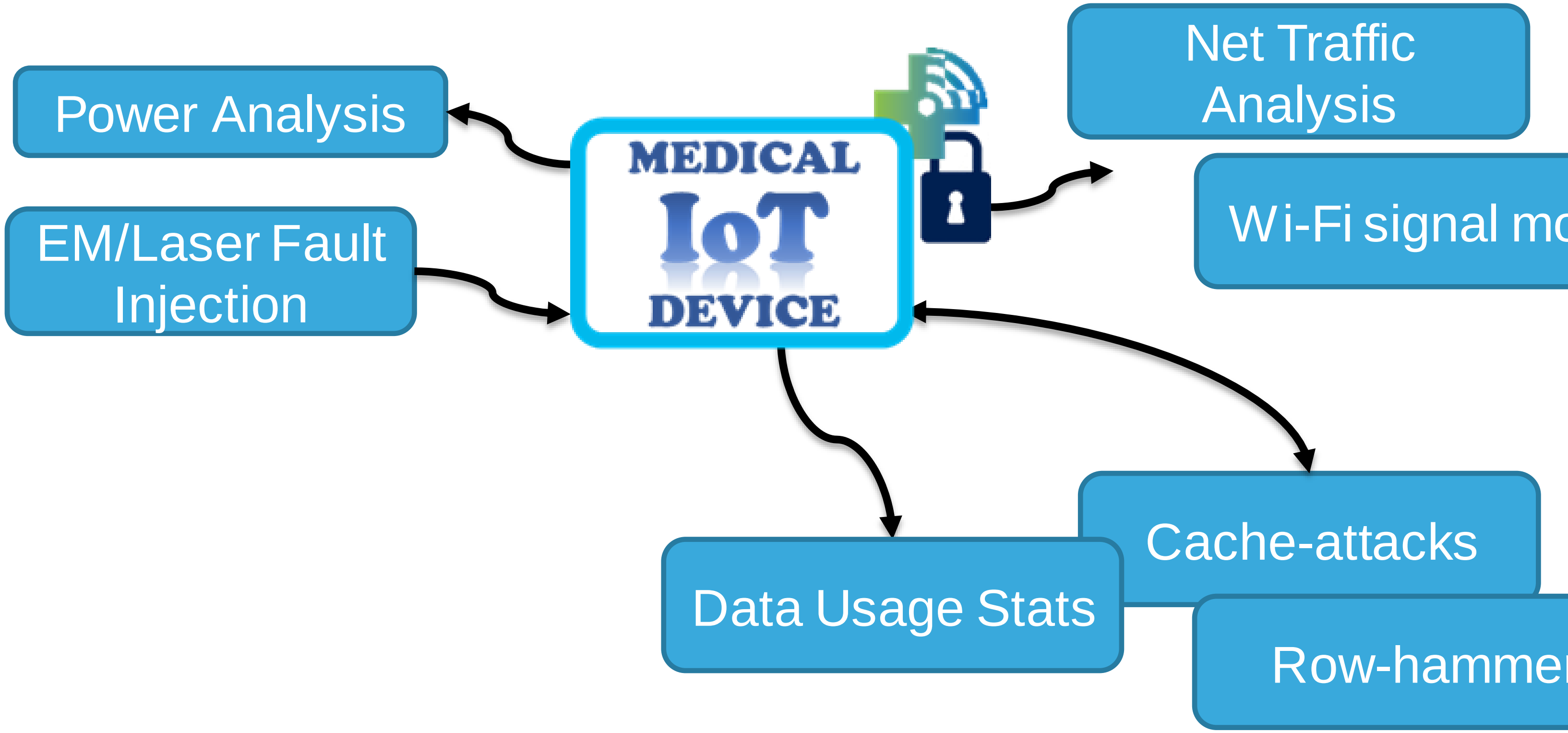


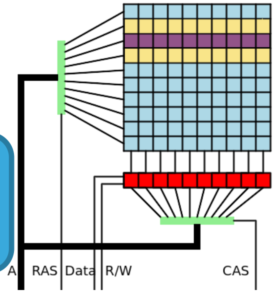


Vicinity: **eavesdrop** target's communication channels



```
~ :-)netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 is233376.intra.ce:33164 74.120.188.194:https    ESTABLISHED
tcp        0      0 is233376.intra.ce:33168 74.120.188.194:https    TIME_WAIT
tcp        0      0 is233376.intra.ce:55238 10.0.224.102:imaps      ESTABLISHED
tcp        0      0 is233376.intra.ce:54430 dzr-viplb-01.ig-1:https ESTABLISHED
tcp        0      0 is233376.intra.ce:33166 74.120.188.194:https    TIME_WAIT
tcp        0      0 is233376.intra.ce:50054 grewprdsfarm1.intr:3389 ESTABLISHED
tcp        0      0 is233376.intra.ce:32888 par10s33-in-f2.1e:https ESTABLISHED
tcp        0      0 is233376.intra.ce:46650 151.101.192.194:http    ESTABLISHED
tcp        0      0 is233376.intra.ce:36672 ec2-176-34-155-23:https ESTABLISHED
tcp        0      0 is233376.intra.ce:33176 74.120.188.194:https    TIME_WAIT
tcp        0      0 is233376.intra.ce:46648 151.101.192.194:http    ESTABLISHED
tcp        0      0 is233376.intra.ce:57270 wl-in-f157.1e100.:https TIME_WAIT
tcp        0      0 is233376.intra.ce:57154 ec2-54-75-239-212:https ESTABLISHED
tcp        0      0 is233376.intra.ce:60808 74.120.188.204:https    ESTABLISHED
tcp        0      0 is233376.intra.ce:36172 151.101.128.194:https   ESTABLISHED
tcp        0      0 is233376.intra.ce:35052 wl-in-f154.1e100.:https ESTABLISHED
tcp        1      0 is233376.intra.ce:53222 grexp009imp.intra.c:ipp CLOSE_WAIT
```





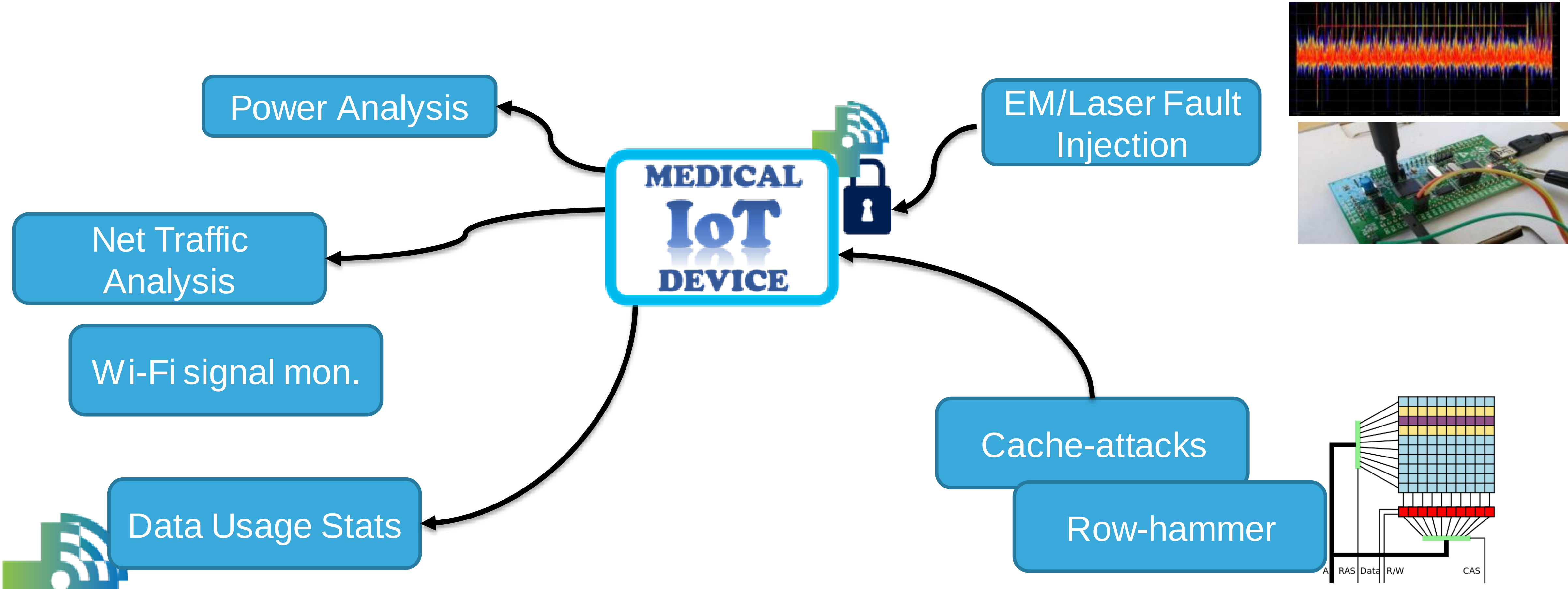
Remote: attacker only relies on **execution of code** on the target

By Dsimic - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php curid=38868341

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

MEDICAL IoT DEVICE

EM/Laser Fault Injection

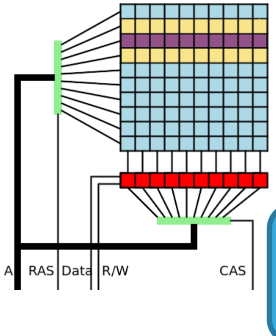
Cache-attacks

Row-hammer

Security of the IoMT Chain

Logical: exploit **software** property

Physical: exploit **hardware** property



Cache-attacks

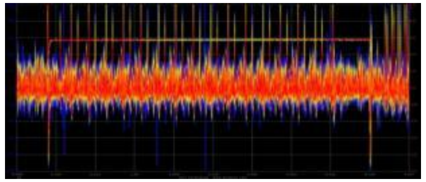
Row-hammer

Net Traffic Analysis

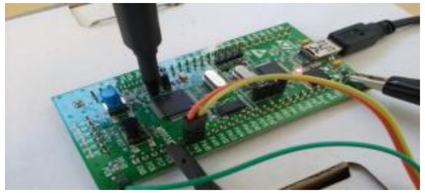
Data Usage Stats

MEDICAL IoT DEVICE

Power Analysis



EM/Laser Fault Injection



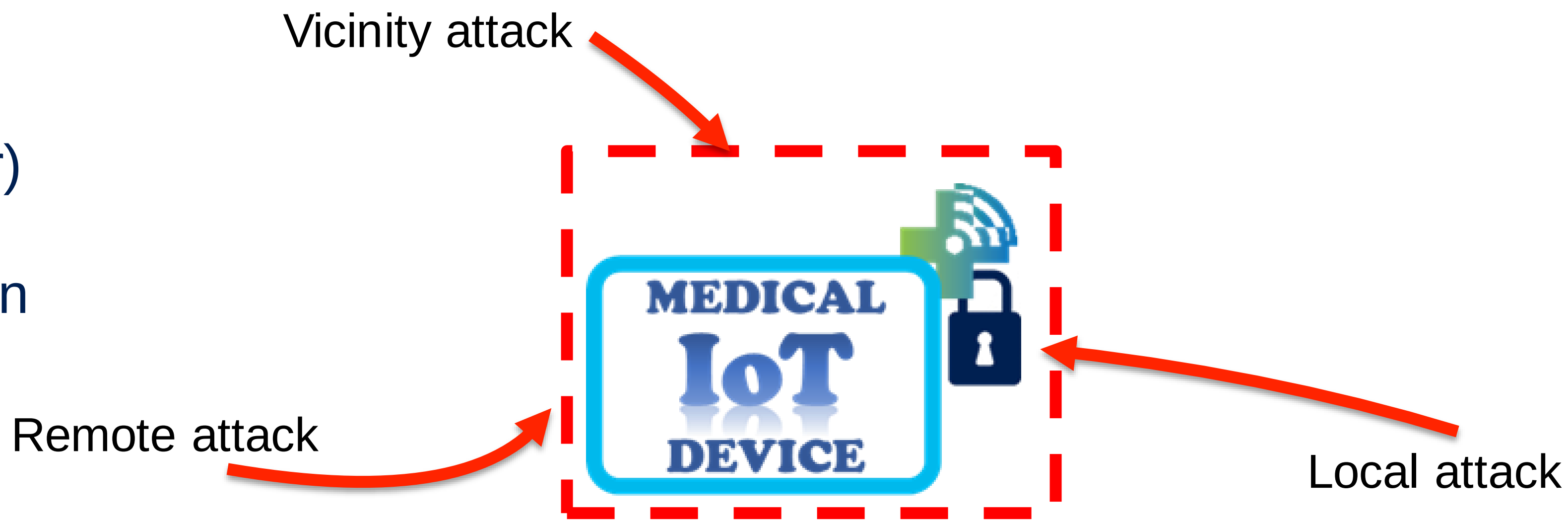
Wi-Fi signal mon.

SERENE IoT

Security of IoMT Devices

Assets

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



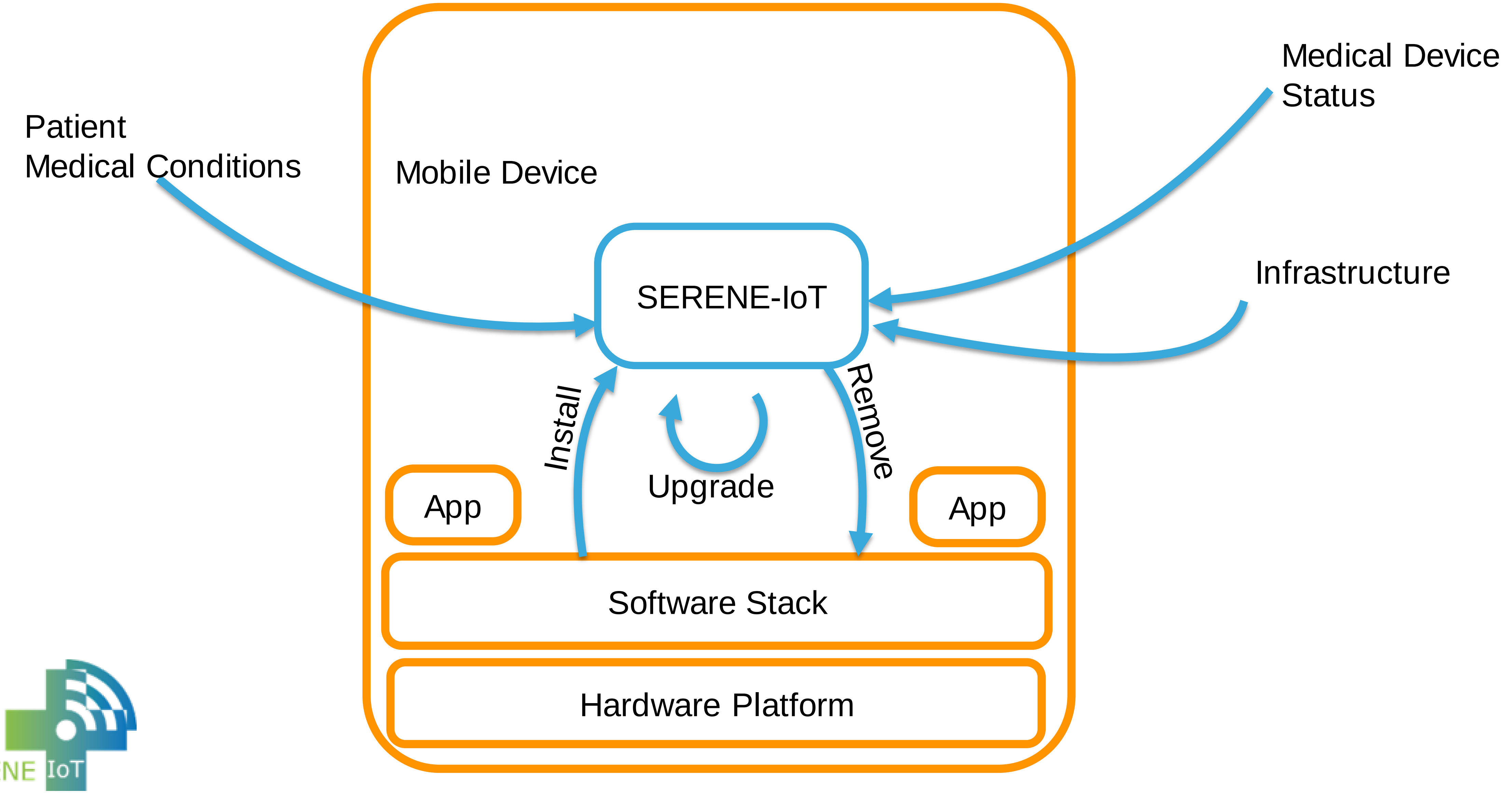
(Security) Risks

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

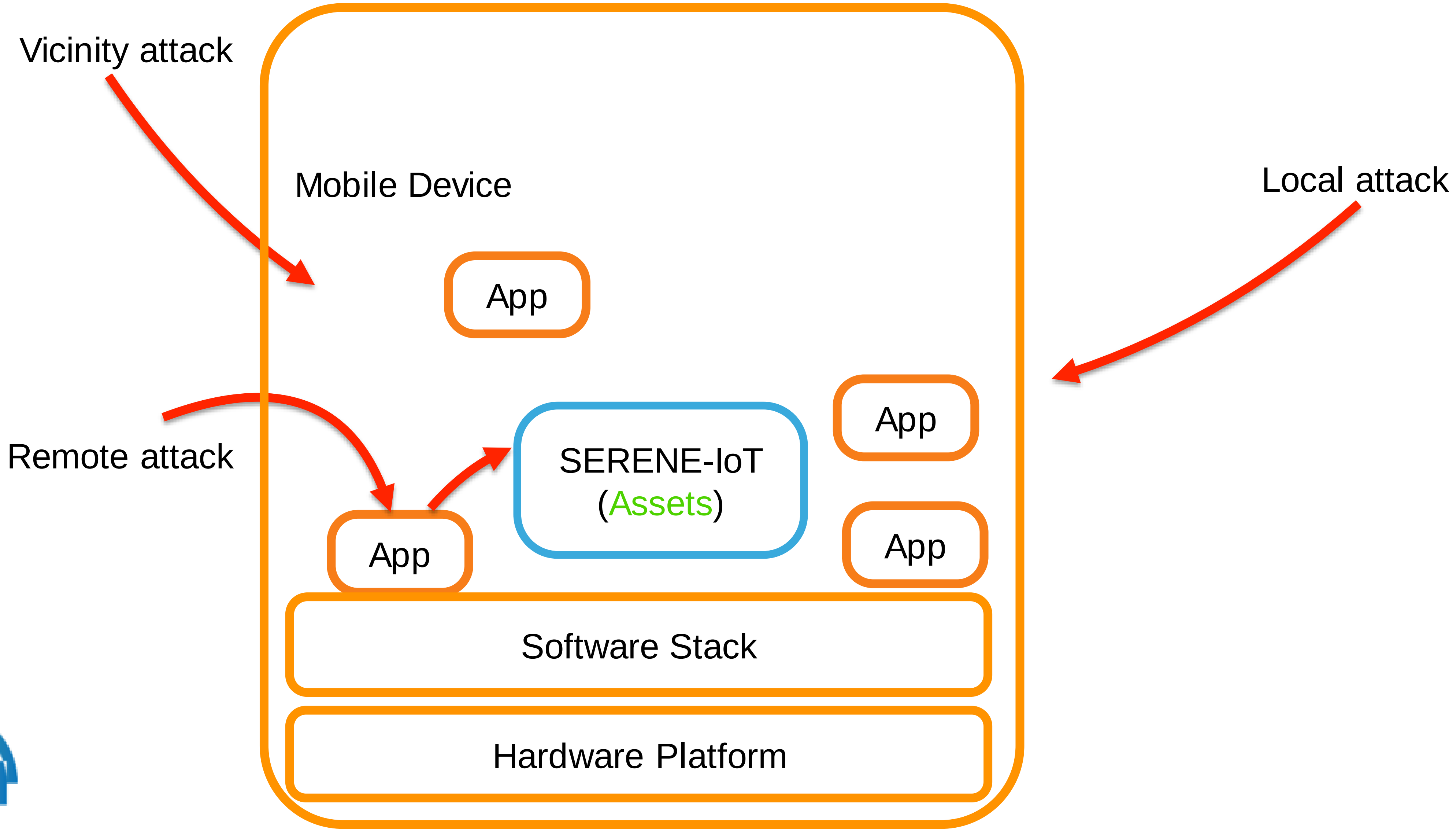
Existing Counter-Measures

- HW: secure elements, shielding
- SW: masking, hiding, obfuscation,

Security of Mobile Applications



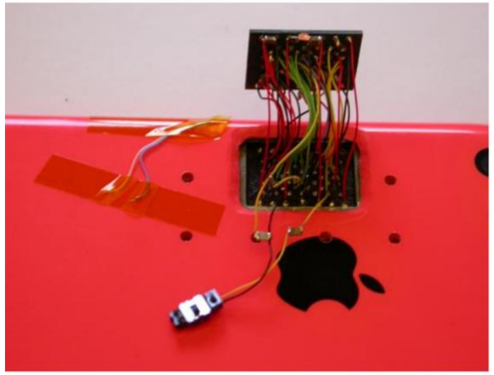
Security of Mobile Applications



Local Attacks on Mobile Platforms

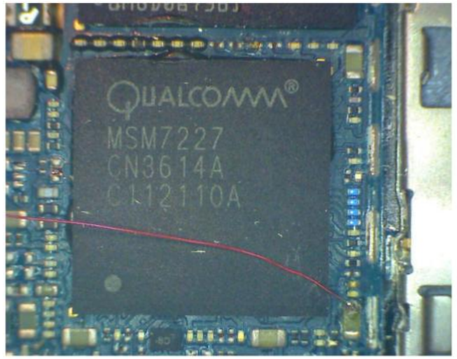
Demonstrated, accessible attacks:

- **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]



[Skorobogatov2015]

[Genkin 2016]



[O'Flynn 2016]

Hard or not-demonstrated attacks:

- **Power-Analysis Attacks**
- **Clock Glitching**
- **Laser Attacks**

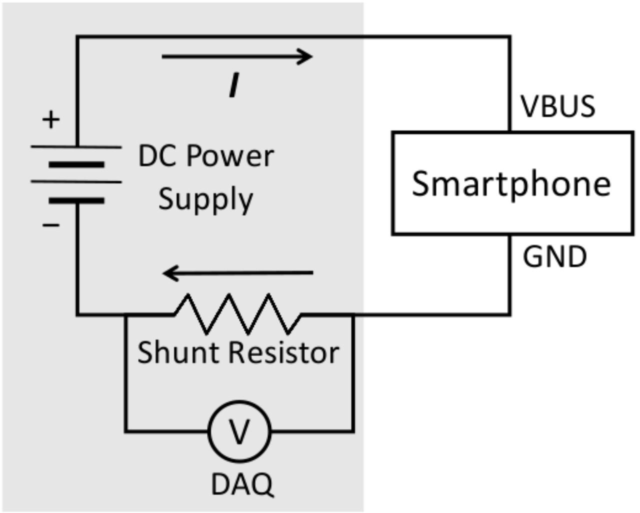
Vicinity Attacks on Mobile Platforms

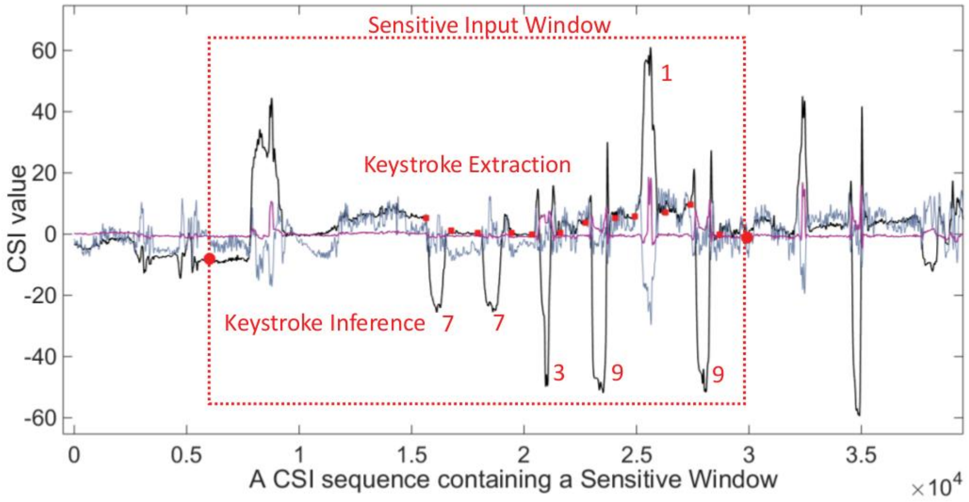
- **Network Analysis** to fingerprint applications [Conti 2016a, Stöber 2013]

- **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 infere browsing behaviors, application transitions *[Jana 2012, Chen 2014]*
  - Observe app's **context switches** and infer finger movements [Simon 2016, Diao 2016]

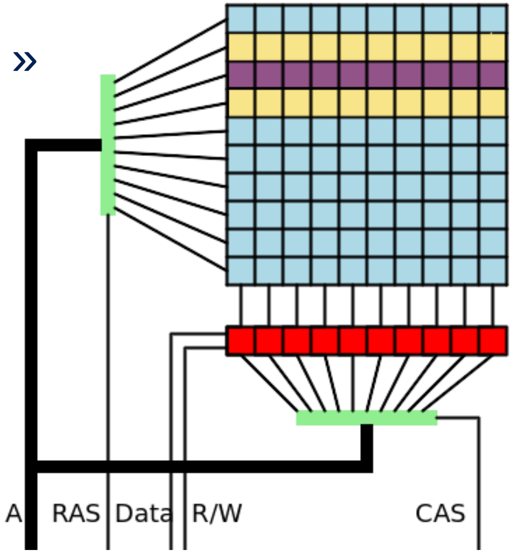
- Observe and force system's **page deduplication** to fingerprint visited website.

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

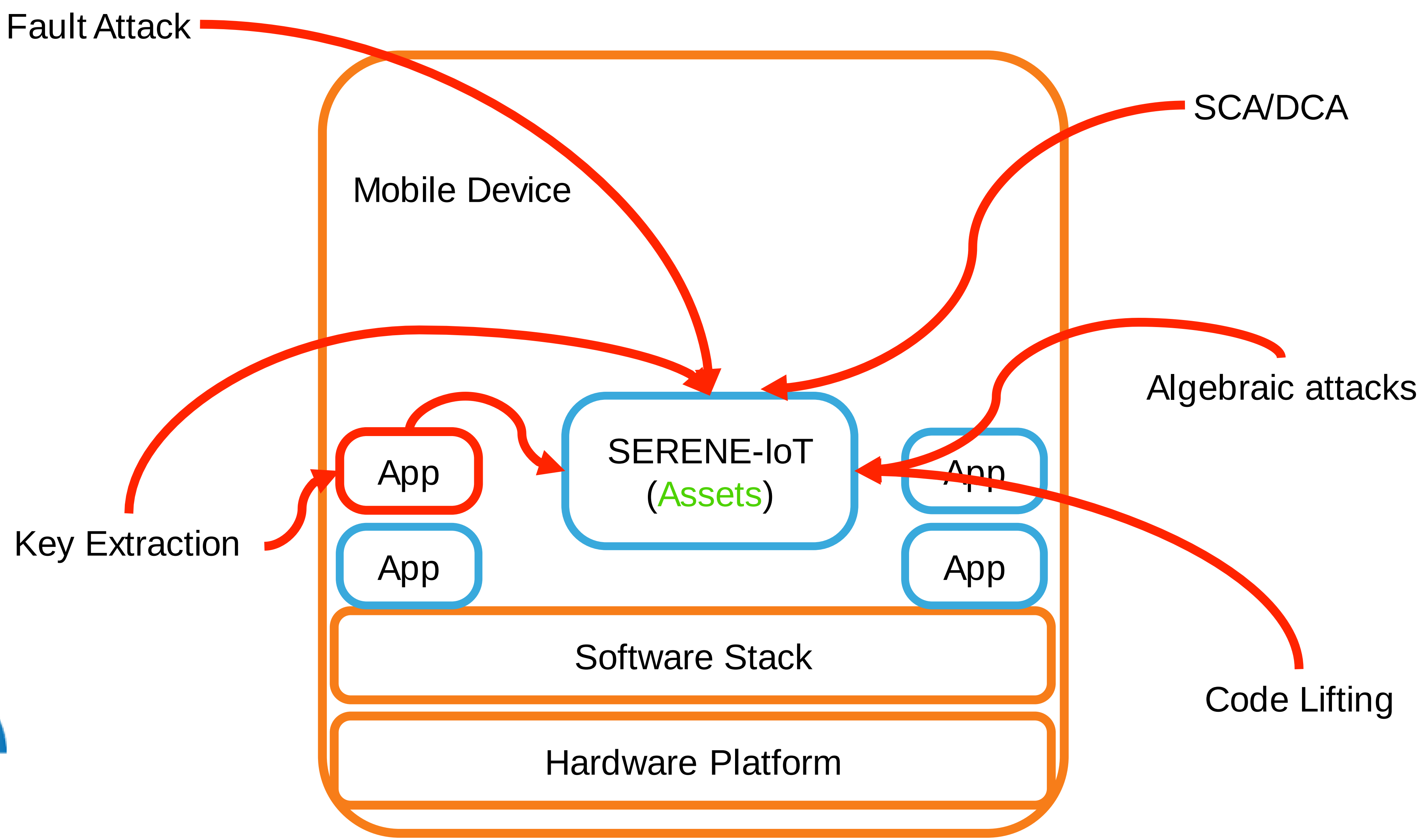
- **RowHammer** : well-chosen memory writes change state of adjacent « logically protected » celles [VanDerVeen 2015, Kim 2014, Seaborn 2015, Gruss 2016]

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

- And of course … **Reverse-engineering**

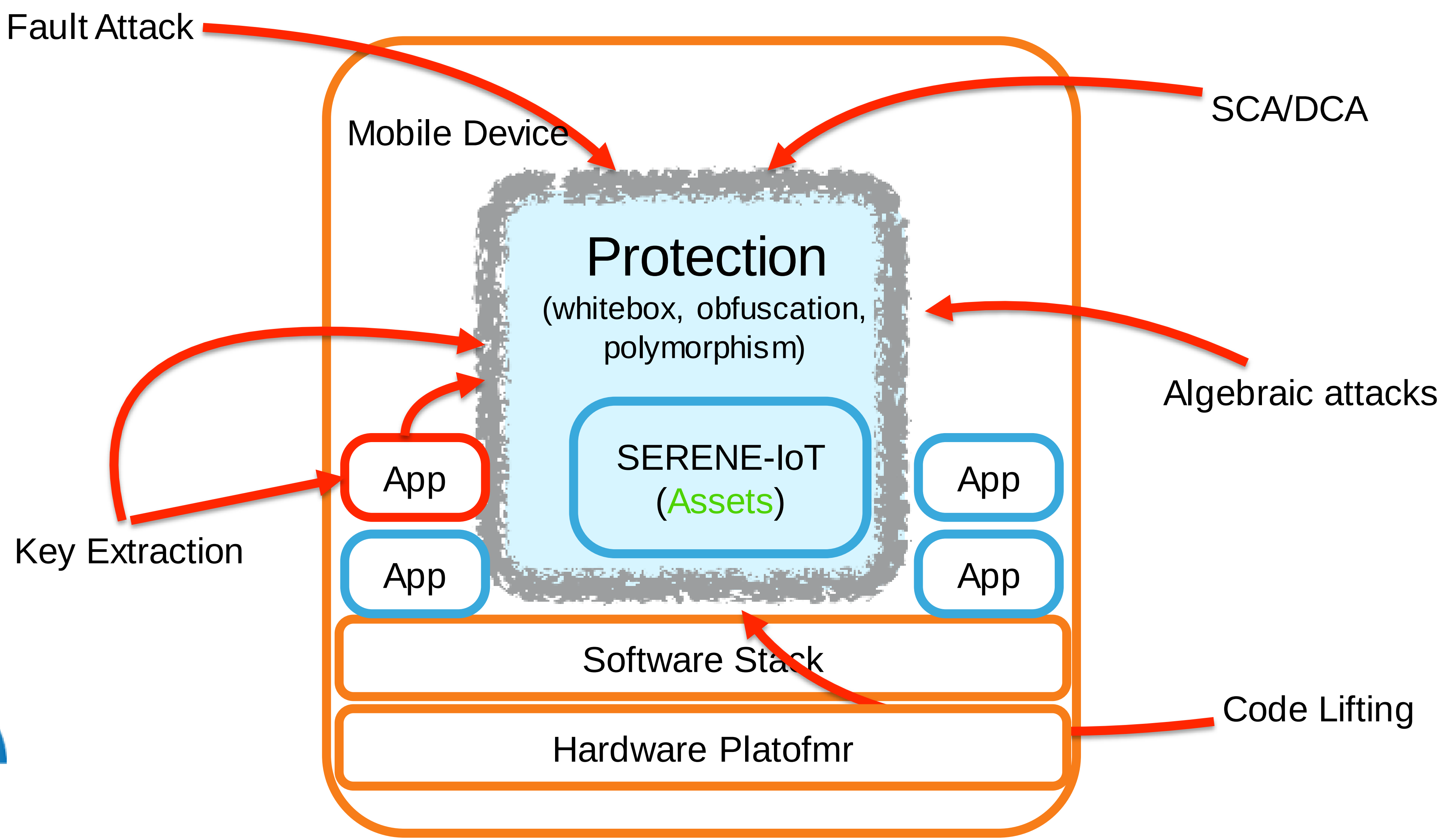


Security of Mobile Applications



SERENE IoT

Security of Mobile Applications



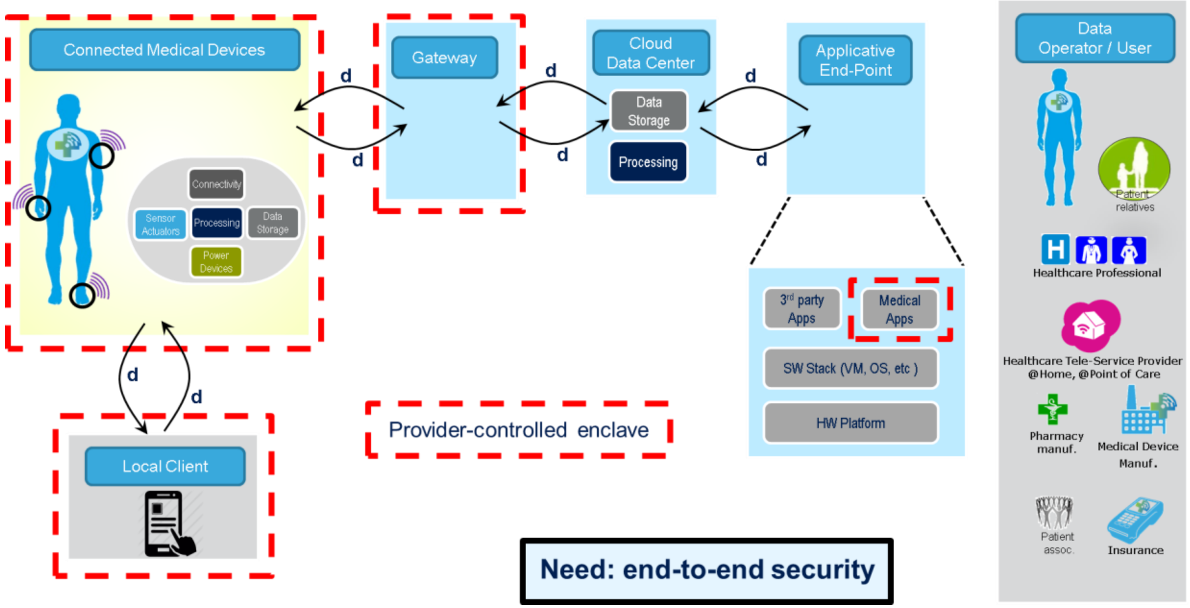
SERENE-IoT: Expected Contributions

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



Need: end-to-end security

SW-level Security

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

SERENE IoT

Conclusion

- IoT is reaching medical devices and applications
- The use of open platforms (smartphone) introduces news 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:
  - Assets and risk identification following and extending *ISO/IEC 27005:2011, Annex A* and *IEC-TR 80001-2-1:2012, Annex D*
  - HW protections against physical attacks
  - SW protections against attacks on mobile applications
  - Use of Blockchain to implement consent management

Selected Bibliography

- **[Spreitzer 2017]** Spreitzer, R.; Moonsamy, V.; Korak, T. & Mangard, S. *Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices* IEEE Communications Surveys & Tutorials, IEEE, 2017
- **[Genkin 2016]** D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, *ECDSA key extraction from mobile devices via nonintrusive physical side channels*, in Proc. Conf. Comput. Commun. Security (CCS), Vienna, Austria, 2016, pp. 1626–1638.
- **[NewAE 2016]** *Fault Injection Raspberry PI*, NewAE Technol. Inc., Halifax, NS, Canada, accessed: Aug. 3, 2016. [Online]. Available: https://wiki.newae.com
- **[Oflynn 2016]** C. O'Flynn, *Fault injection using crowbars on embedded systems*, IACR Cryptology ePrint Archive, Report 2016/810, 2016. [Online]. Available: https://eprint.iacr.org/2016/810
- **[Rivier 2016]** L. Rivière et al., *High precision fault injections on the instruction cache of ARMv7-M architectures*, in Proc. Hardw. Orient. Security Trust (HOST), Washington, DC, USA, 2015, pp. 62–67.
- **[Ordas 2017]** S. Ordas, L. Guillaume-Sage, and P. Maurine, *Electromagnetic fault injection: The curse of flip-flops*, J. Cryptograph. Eng., vol. 7, no. 3, pp. 183–197, 2017.
- **[Skorobogatov 2015]** S. Skorobogatov, *The bumpy road towards iPhone 5c NAND mirroring*, arXiv ePrint Archive, Report 1609.04327, 2016. [Online]. Available: https://arxiv.org/abs/1609.04327
- **[Conti 2016a]** M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, *Analyzing Android encrypted network traffic to identify user actions*, IEEE Trans. Inf. Forensics Security, vol. 11, no. 1, pp. 114–125, Jan. 2016.
- **[Stober 2013]** T. Stöber, M. Frank, J. B. Schmitt, and I. Martinovic, *Who do you sync you are?: Smartphone fingerprinting via application behaviour*, in Proc. Security Privacy Wireless Mobile Netw. (WISEC), Budapest, Hungary, 2013, pp. 7–12.
- **[Yang 2017]** Q. Yang, P. Gasti, G. Zhou, A. Farajidavar, and K. S. Balagani, *On inferring browsing activity on smartphones via USB power analysis side-channel*, IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1056–1066, May 2017.
- **[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), Xi'an, China, 2016, pp. 37–44.
- **[Ali 2015]** K. Ali, A. X. Liu, W. Wang, and M. Shahzad, *Keystroke recognition using WiFi signals*, in Proc. Mobile Comput. Netw. (MOBICOM), Paris, France, 2015, pp. 90–102.
- **[Zhang 2016]** J. Zhang et al., *Privacy leakage in mobile sensing: Your unlock passwords can be leaked through wireless hotspot functionality*, Mobile Inf. Syst., vol. 2016, pp. 1–14, Mar. 2016.
- **[Li 2016]** M. Li et al., *When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals*, in Proc. Conf. Comput. Commun. Security (CCS), Vienna, Austria, 2016, pp. 1068–1079
- **[He 2014]** G. He, M. Yang, X. Gu, J. Luo, and Y. Ma, *A novel active website fingerprinting attack against Tor anonymous system*, in Proc. Comput. Supported Cooperative Work Design (CSCWD), Hsinchu, Taiwan, 2014, pp. 112–117.
- **[Jana 2012]** S. Jana and V. Shmatikov, *Memento: Learning secrets from process footprints*, in Proc. IEEE Symp. Security Privacy (S P), San Francisco, CA, USA, 2012, pp. 143–157
- **[Chen 2014]** Q. A. Chen, Z. Qian, and Z. M. Mao, *Peeking into your app without actually seeing it: UI state inference and novel Android attacks*, in Proc. USENIX Security Symp., San Diego, CA, USA, 2014, pp. 1037–1052.

Selected Bibliography

- **[Simon 2016]** L. Simon, W. Xu, and R. Anderson, *Don’t interrupt me while I type: Inferring text entered through gesture typing on Android keyboards*, Proc. Privacy Enhancing Technol., vol. 2016, no. 3, pp. 136–154, 2016.
- **[Diao 2016]** W. Diao, X. Liu, Z. Li, and K. Zhang, *No pardon for the interruption: New inference attacks on Android through interrupt timing analysis*, in Proc. IEEE Symp. Security Privacy (S P), San Jose, CA, USA, 2016, pp. 414–432.
- **[Ge 2016]** Q. Ge, Y. Yarom, D. Cock, and G. Heiser, *A survey of microarchitectural timing attacks and countermeasures on contemporary hardware*, J. Cryptograph. Eng., pp. 1–27, 2016.
- **[Szefer 2016]** J. Szefer, *Survey of microarchitectural side and covert channels, attacks, and defenses*, IACR Cryptology ePrint Archive, Report 2016/479, 2016. [Online]. Available: https://eprint.iacr.org/2016/479
- **[VanDerVeen 2015]** V. van der Veen et al., *Drammer: Deterministic rowhammer attacks on mobile platforms*, in Proc. Conf. Comput. Commun. Security (CCS), Vienna, Austria, 2016, pp. 1675–1689.
- **[Kim 2014]** Y. Kim et al., *Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors*, in Proc. Int. Symp. Comput. Archit. (ISCA), Minneapolis, MN, USA, 2014, pp. 361–372.
- **[Seaborn 2015]** M. Seaborn and T. Dullien, *Exploiting the DRAM rowhammer bug to gain kernel privileges*, Blackhat, 2015. [Online]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Seaborn-Exploiting-The-DRAM-Rowhammer-Bug-To-Gain-Kernel-Privileges.pdf
- **[Gruss 2016]** D. Gruss, C. Maurice, and S. Mangard, *Rowhammer.js: A remote software-induced fault attack in JavaScript*, in Detection of Intrusions and Malware & Vulnerability Assessment—DIMVA (LNCS 9721). Cham, Switzerland: Springer, 2016, pp. 300–321.
- **[Bos 2016]** J. W. Bos, C. Hubain, W. Michiels, and P. Teuwen, *Differential computation analysis: Hiding your white-box designs is not enough*, in Cryptographic Hardware and Embedded Systems—CHES 2016 (LNCS 9813). Heidelberg, Germany: Springer, 2016, pp. 215–236.