www.crysys.hu

SETIT

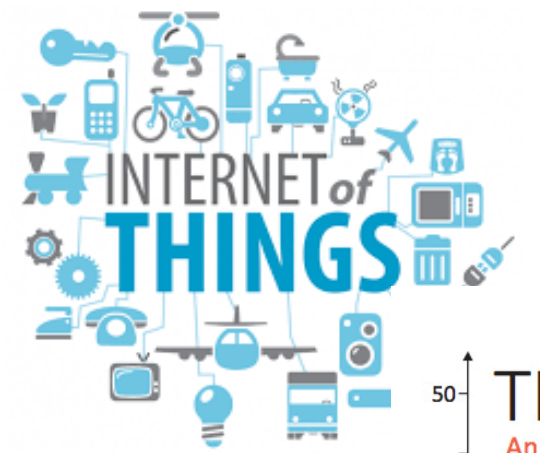
Security Enhancing Technologies for the Internet of Things

Levente Buttyán

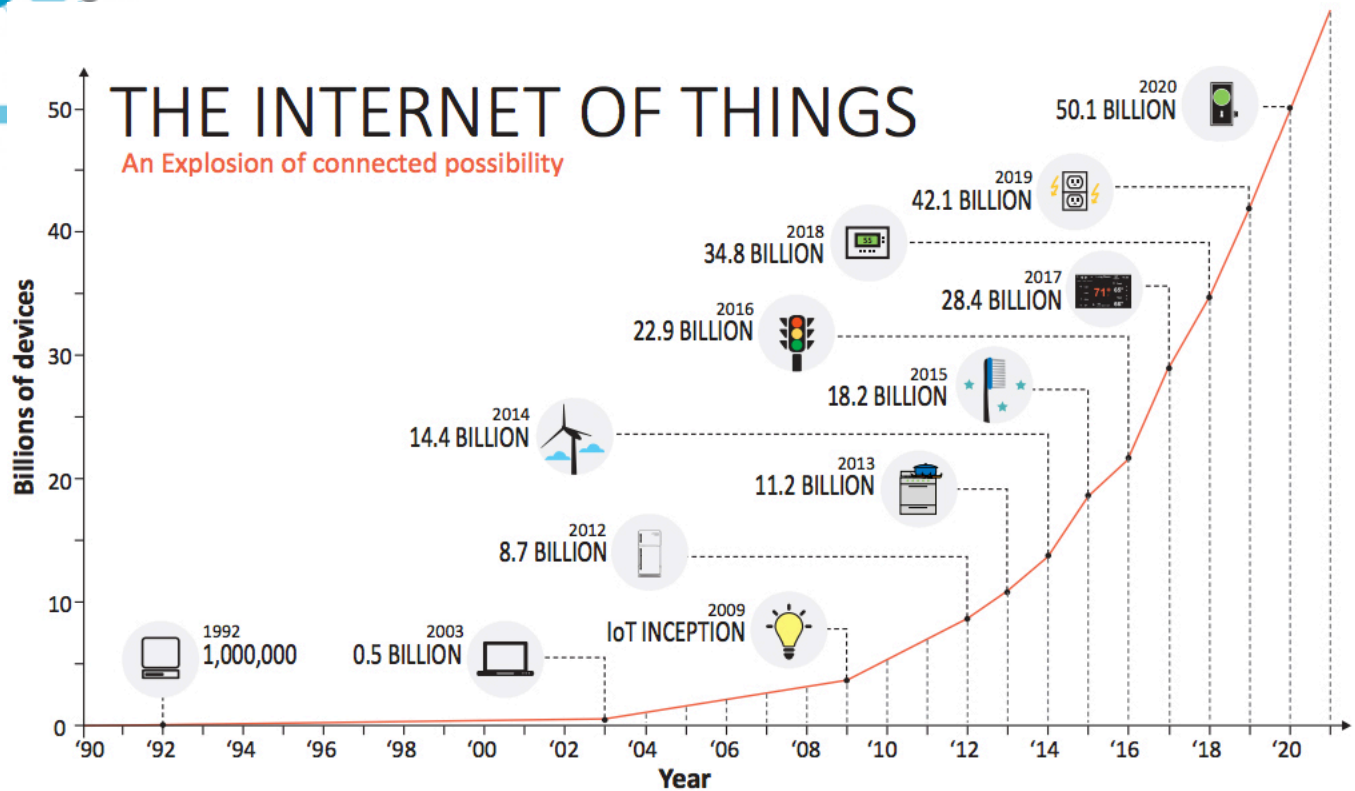
CrySyS Lab, BME

buttyan@crysys.hu

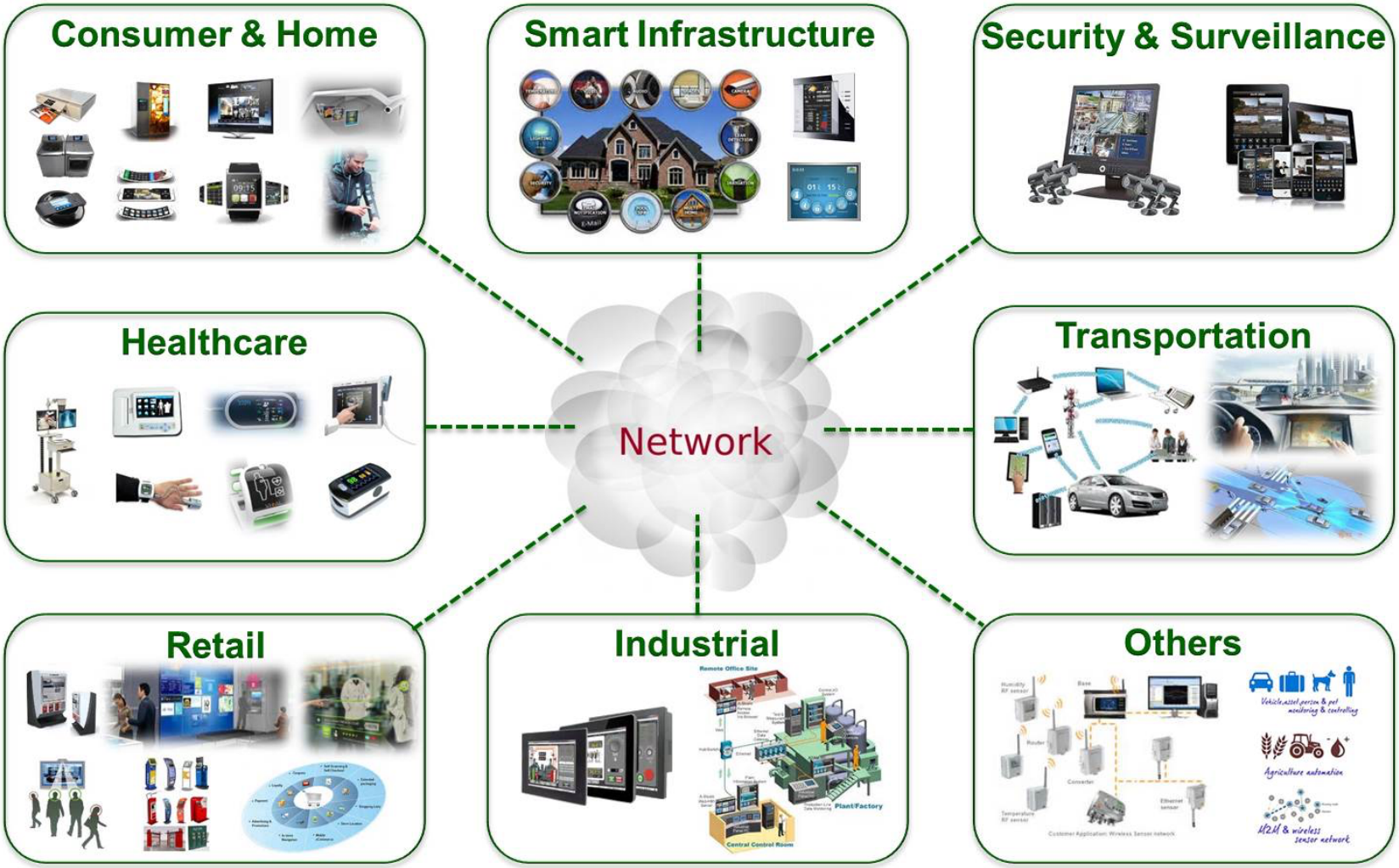
Internet of Things



Embedded devices connected to the Internet…



IoT applications



How about security?

SECURITY

No surprise, IoT devices are insecure

By

Hacking a living room: Kaspersky Lab researcher finds

Report: Cars are vulnerable to wireless hacking

David Shepardson, Detroit New

ENTREPRENEURS 8/03/2013 @ 8:08PM | 15,132 views

PODCASTS

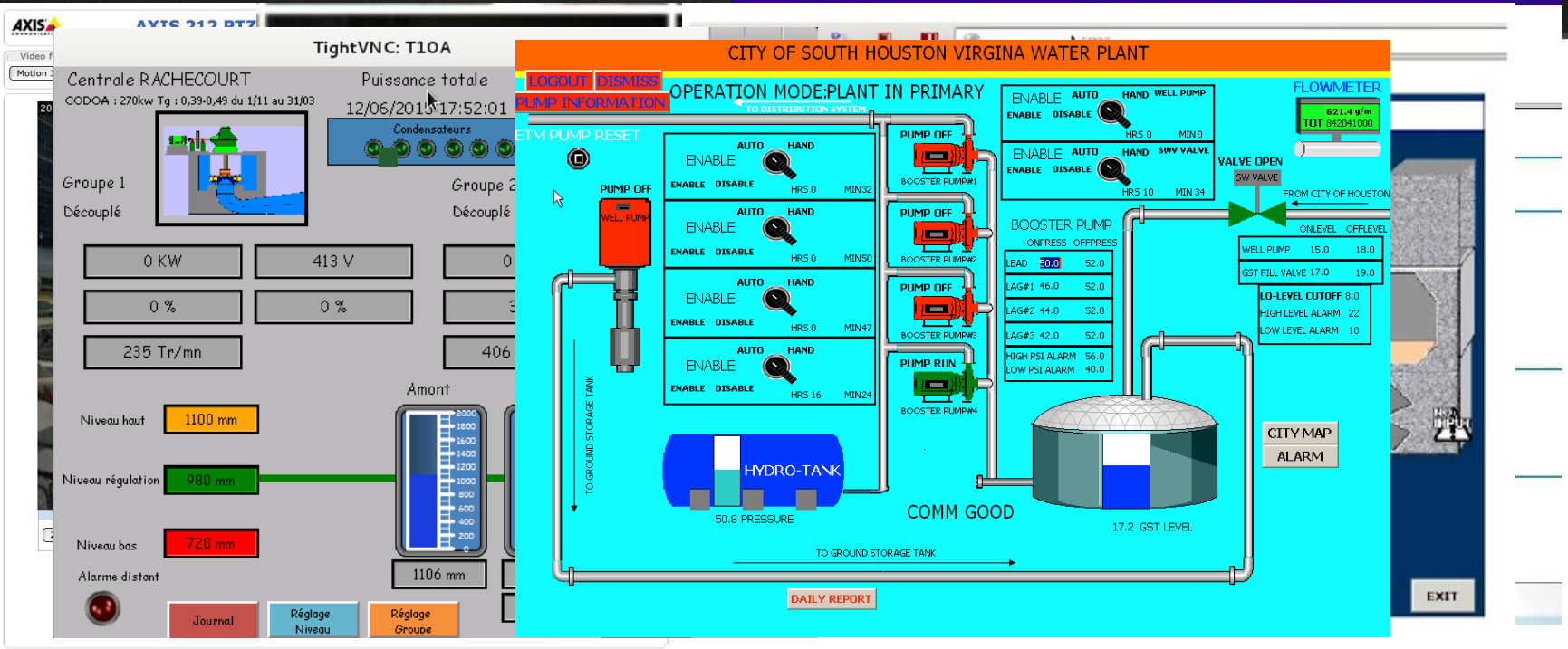
Hacking Insulin Pumps And Other Medical Devices From Black Hat

+ Comment Now + Follow Comments

(Photo: Detroit News, me)

Connected cars aren't the only transportation innovation that's coming down the pike (pun intended). As we've noted before: smart roads and smart infrastructure promise even more transformative changes than – say – having Siri read your text messages to you through your stereo system.

How about security?



Consequences

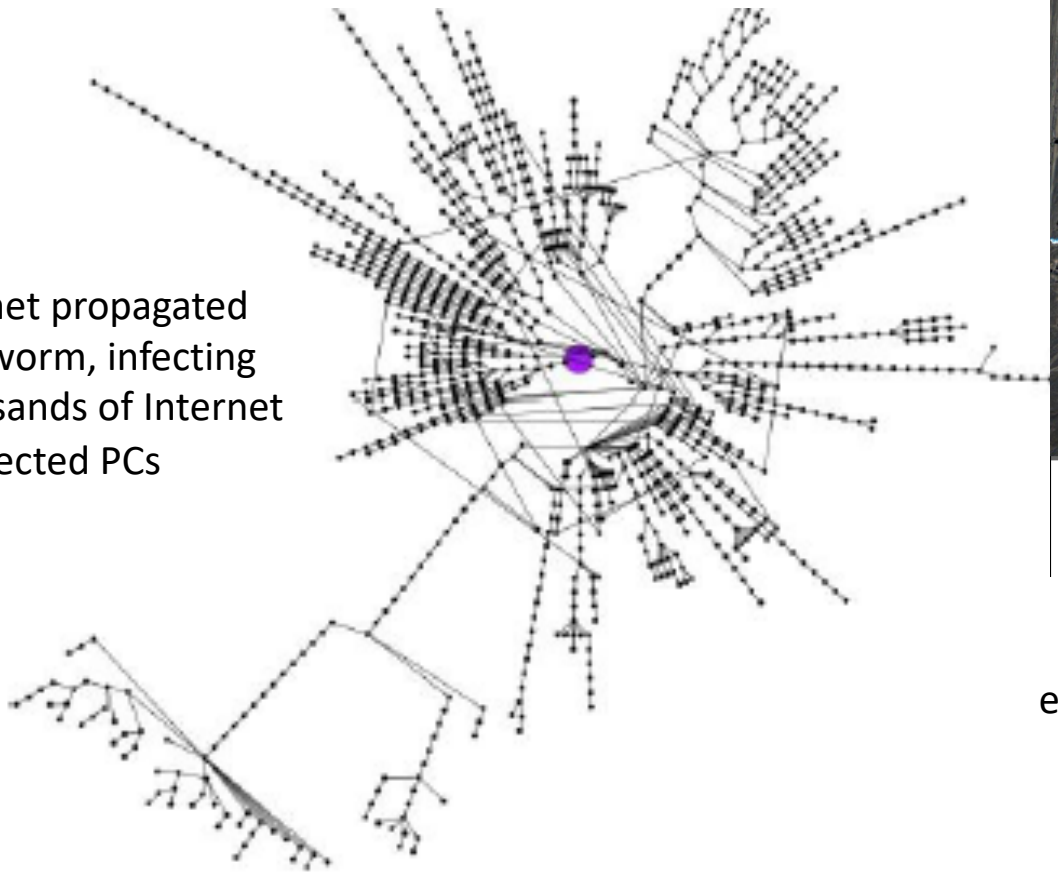
”Traditional” Internet

attacks

attacks

Internet → IoT example: Stuxnet

Stuxnet propagated as a worm, infecting thousands of Internet connected PCs



Once inside the target environment, it reprogrammed PLCs controlling the rotation speed of uranium centrifuges

IoT → Internet example: Mirai botnet

PCWorld
FROM IDG

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS

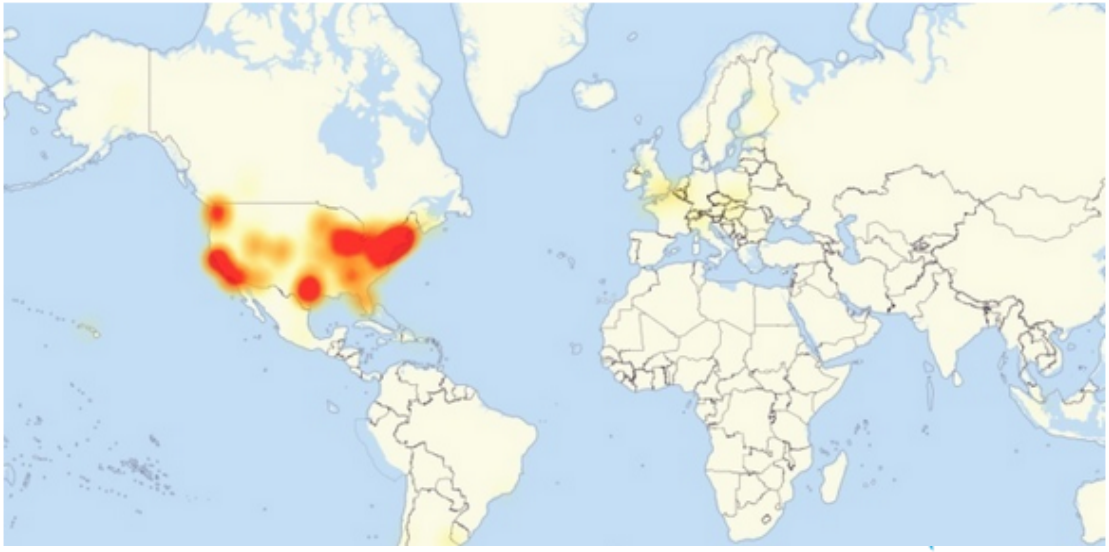
Major DDoS attack knocks Spotify, Twi PayPal, and more o

The sound of silence.

Brad Chacos | *@BradChacos* Oct 21, 2016 3:34
Senior Editor, PCWorld

An IoT botnet is partly behind Friday's massive DDOS attack

DVRs and other devices compromised with the Mirai malware are being the attack.



Michael Kan Oct 21, 2016 4:21 PM
IDG News Service

SETIT project (2018-1.2.1-NKP-2018-00004)

- Goal:
  - Develop new methods (algorithms, protocols, tools, …) that enhance the security of IoT systems

- Research areas:
  - Application level security for embedded devices
  - Platform level security for embedded devices
  - Algebraic foundations and cryptographic building blocks

- Consortium:
  - BME
  - SzTE
  - DE

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
AZ INNOVÁCIÓ LENDÜLETE
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

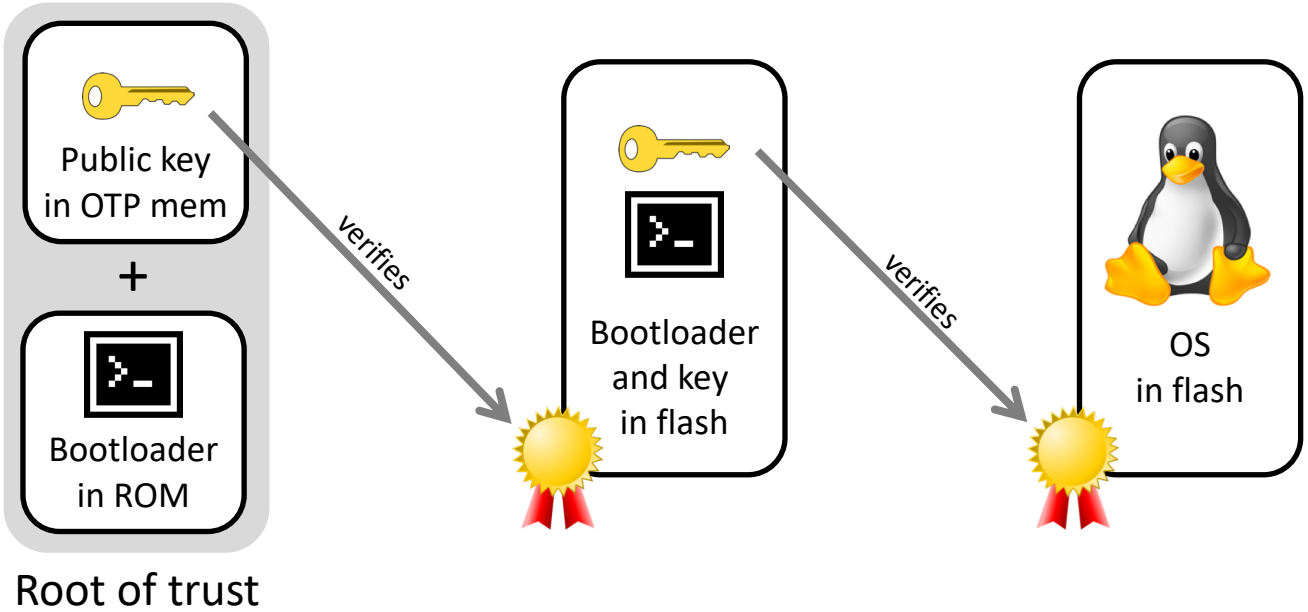
Platform level security for IoT devices

- Can IoT devices be made more difficult to compromise while still keeping their price low?

- Basic ingredients for security:
  - Verified boot
  - Trusted Execution Environment
  - Continuous integrity monitoring
  - Periodic remote attestation of state
  - Secure remote software update

Verified boot

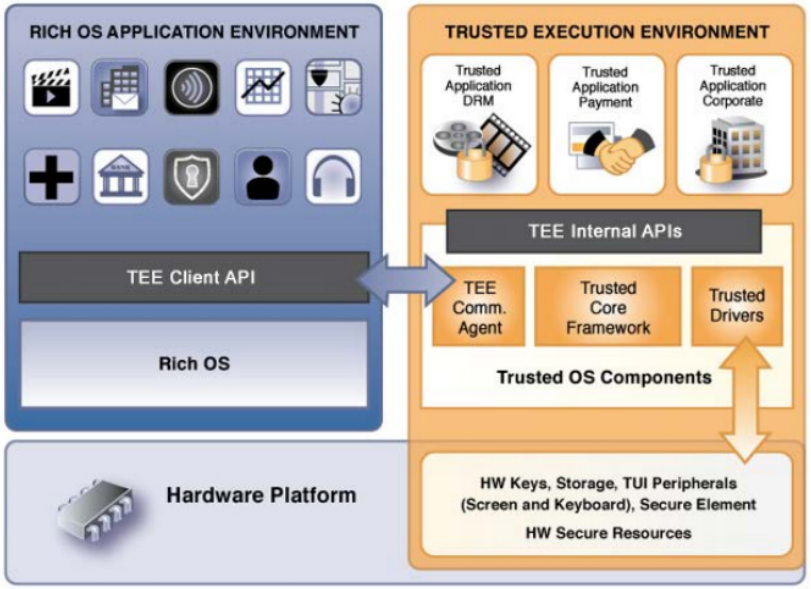
- Brings the device into a known secure state after reset
- Requires digitally signed software components
- Relies on a *chain of trust*



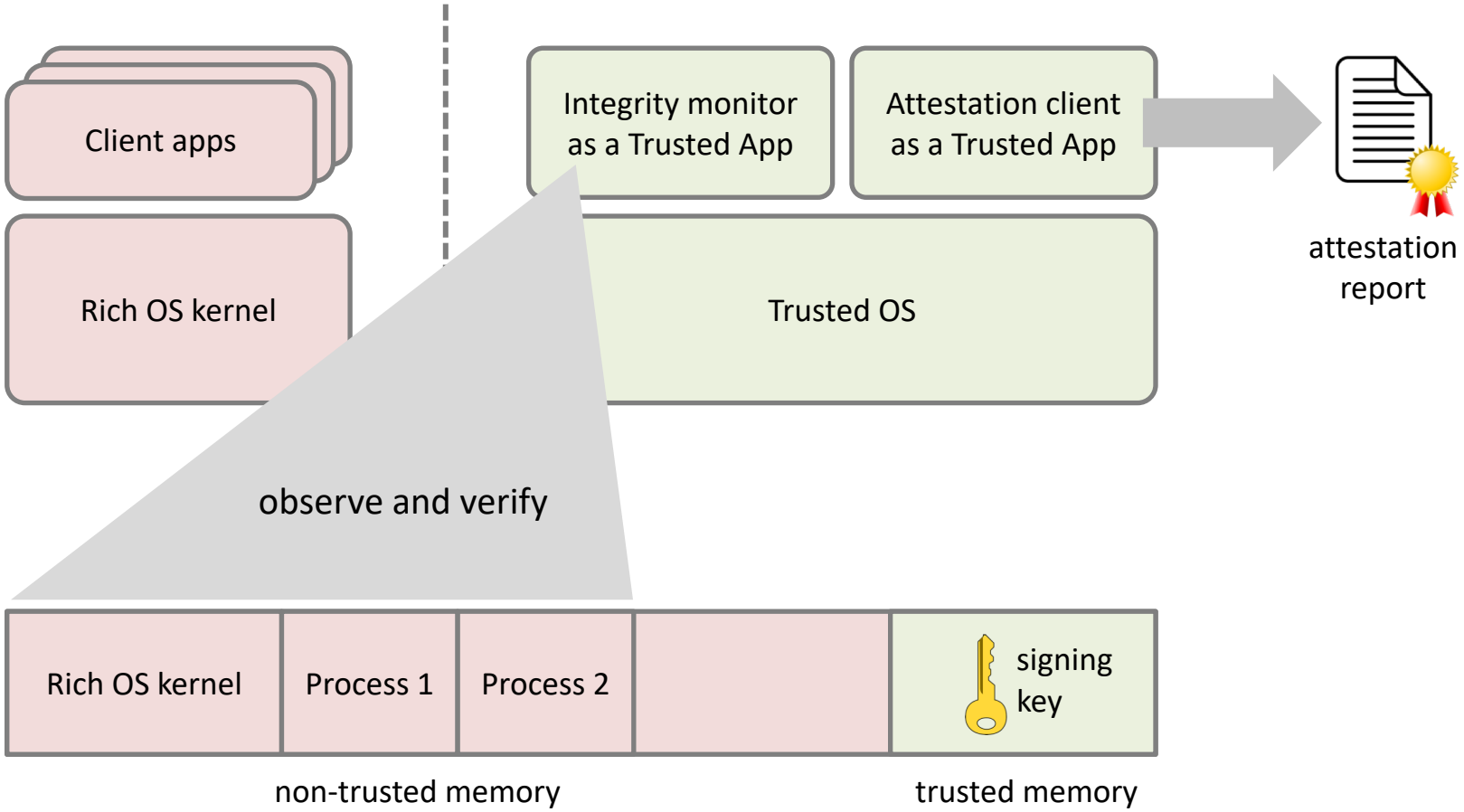
Trusted Execution Environment (TEE)

An isolated execution environment that provides security features such as integrity of applications and confidentiality of their data

- implemented on the main processor (---» performance)
- software based solutions with hardware support for isolation guarantees (---» security)



Integrity monitoring and remote attestation



Secure remote software update

- Needed to fix vulnerabilities discovered during device lifetime
- Software updates are digitally signed
- Software updates are downloaded and installed at next boot
- Update process must be fail safe
- An attacker should not be able to force rollback to a previous (potentially vulnerable) version

Take away messages

- IoT enables interesting, new applications, but poor security of IoT systems can be a road block
- In the SETIT project, we work on removing this road block by developing security enhancing technologies for IoT
- We believe that it is possible to build secure embedded computing platforms at reasonable cost, and we will prove it!

Levente Buttyán
buttyan@crysys.hu