www.crysys.hu

Security of IoT Systems

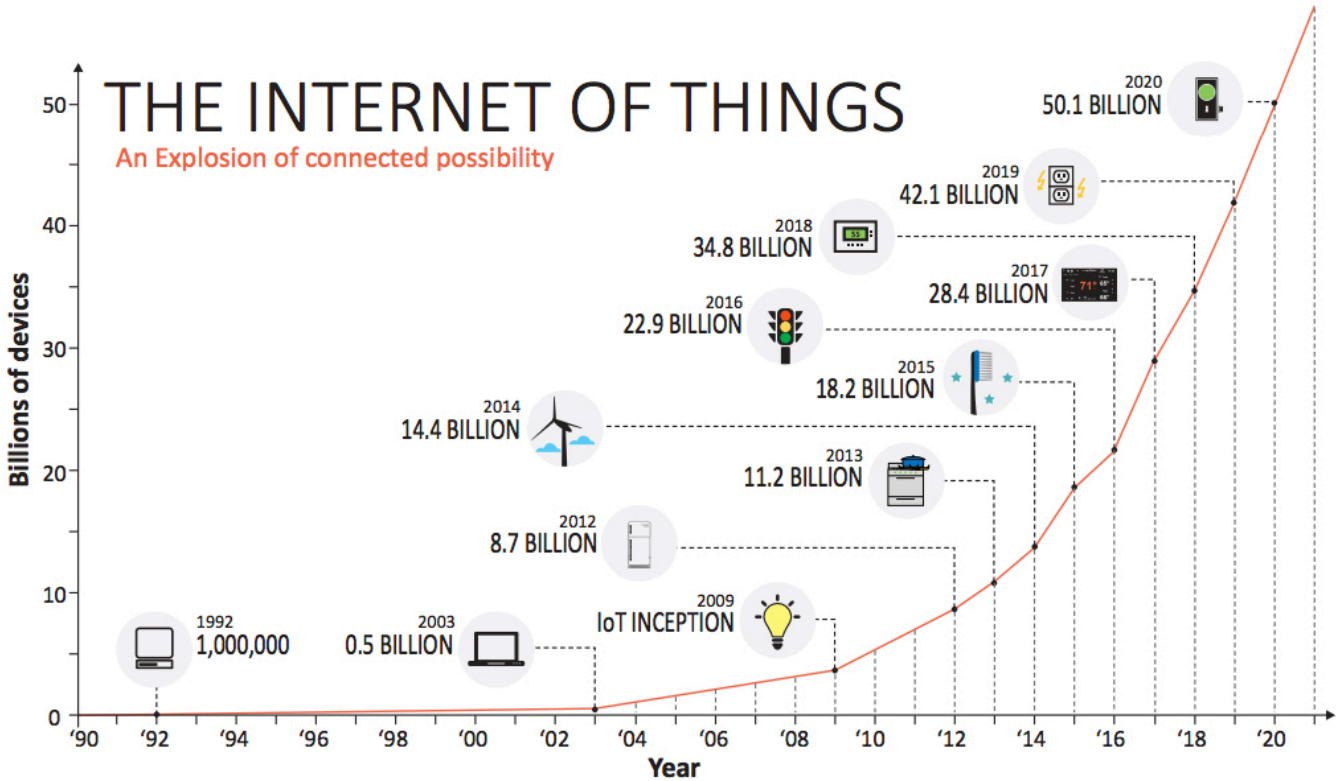
Levente Buttyán

CrySyS Lab, BME

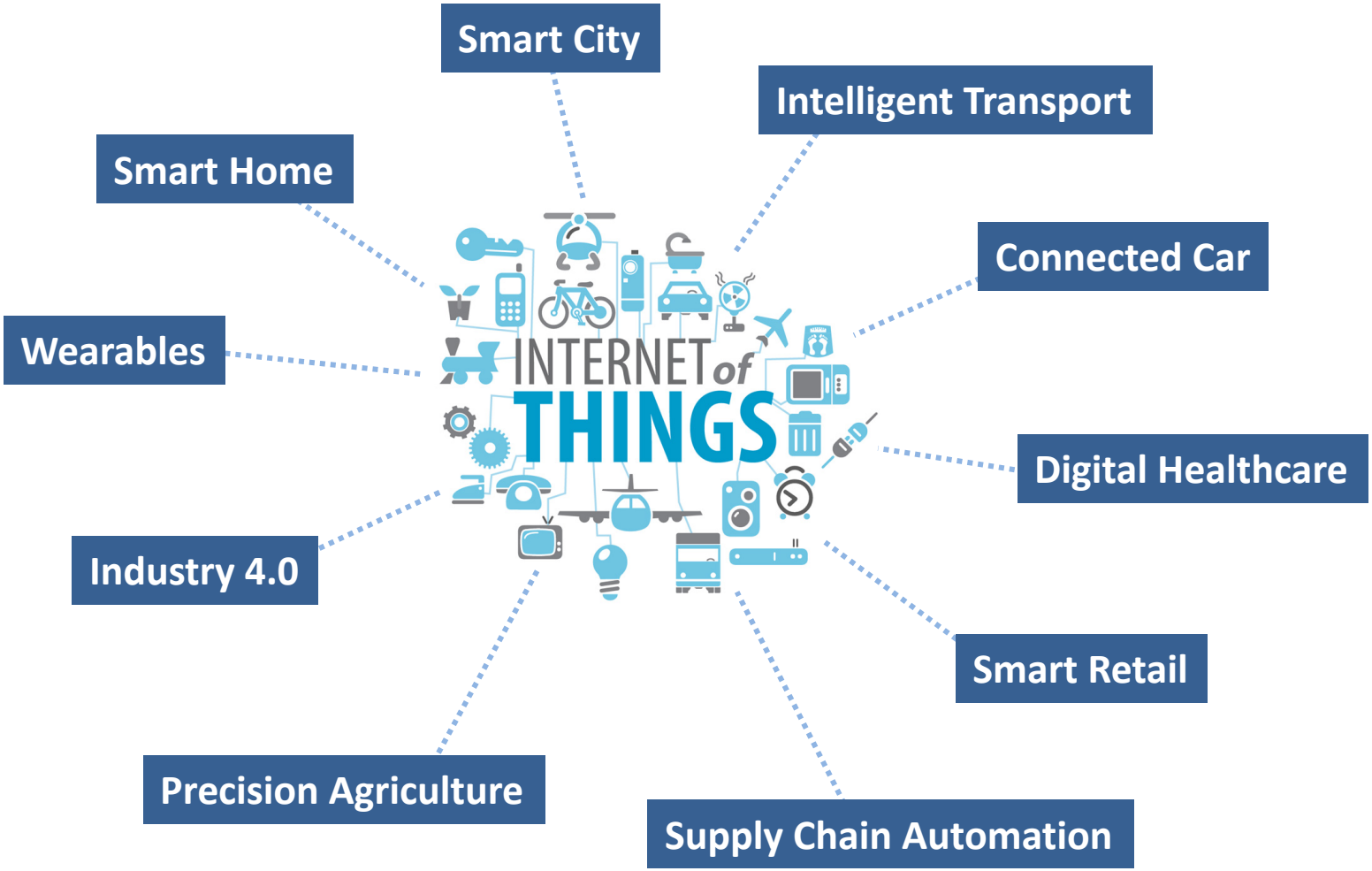
buttyan@crysys.hu

Internet of Things

Embedded devices connected to the Internet



Popular IoT applications



How about security?

The internet of things can be hacked – and the risks are growing every day

By Nicholas Fearn February 12, 2017

techradar

How about security?

threat post

2 Mi
Cor

Somebody's Watching: H
Ring Home Securit

Give Hackers
to

TECHNEWSWORLD

The int
th

Your Smart
dow on

and
ch

ckers Remotely Kill a Jeep on
—With Me in It

WIRED

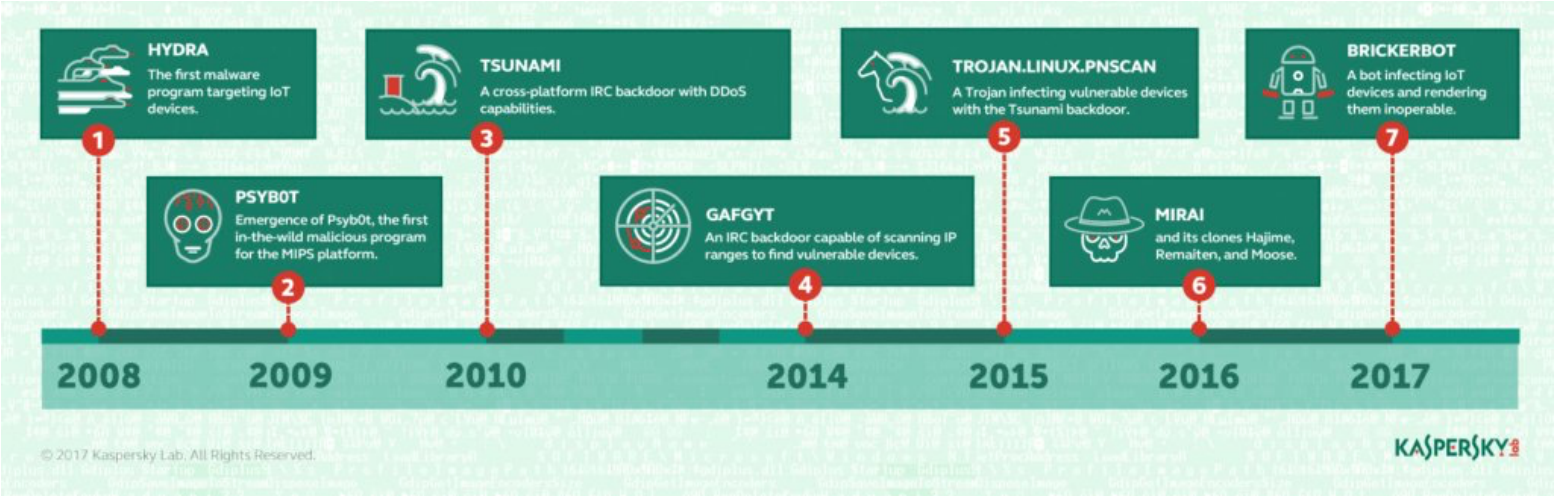
The New York Times

Insulin pumps are vulnerable to hacking,
FDA warns amid recall

The Washington Post

IoT malware

- malware = malicious software
  - generic term that encompasses viruses, worms, Trojans, …
- intrusive code implementing unwanted functions
  - installed without consent of the user
  - performs operations that are not intended by the user

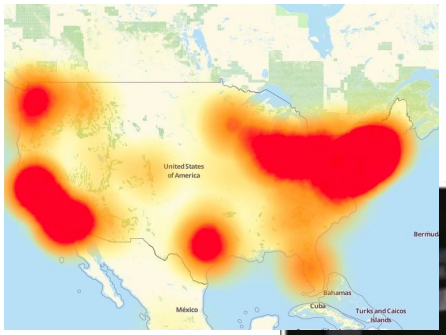


Why targeting IoT?

- It's technically possible
  - IoT devices are (re)programmable --» they can run (malicious) code
- It makes sense economically
  - number of IoT devices is huge and still growing
  - IoT devices are almost always on and connected
  - IoT devices are valuable targets
  - IoT devices are not so esoteric
  - IoT devices are not (yet) designed with security in mind
  - IoT devices are (usually) not operated with security in mind
  - vulnerable devices are easy to find (e.g., with shodan.io)
  - device compromise is hard to detect

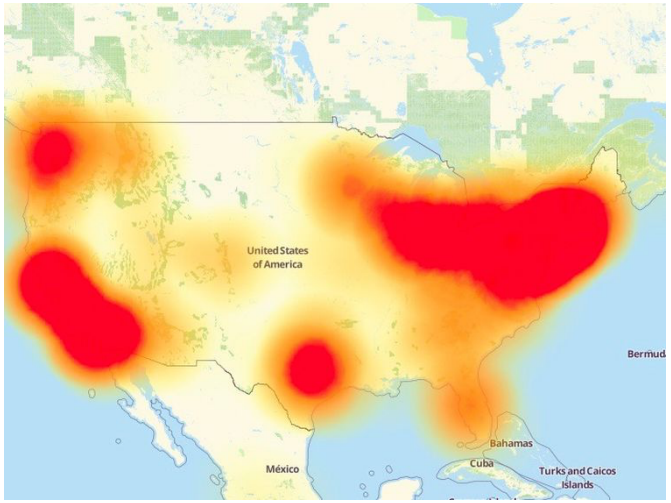
Potential consequences

- IoT botnets can launch massive DDoS attacks on Internet based services
- Infected IoT devices can cause massive privacy breaches
- Cyber attacks on IoT devices in *cyber-physical systems* may cause physical damage or fatal accidents

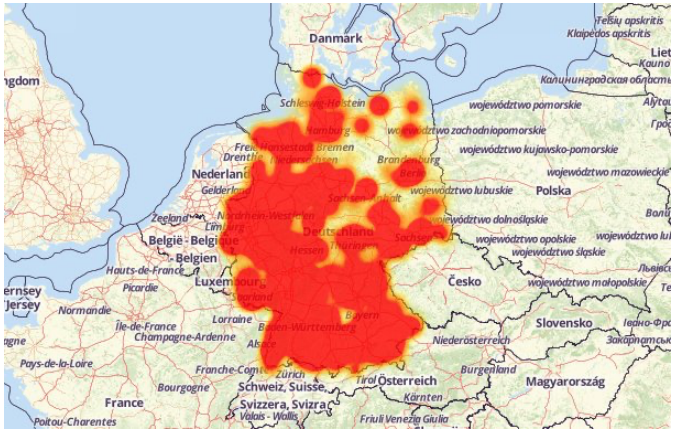


Real-world example – the Mirai botnet

- On 21st October 2016
  - Dyn experienced a DDoS attack on their managed DNS servers
  - the attack was launched by ~100 000 Internet enabled IoT devices, all infected by the Mirai malware
  - according to some experts, the attack magnitude reached 1.2 Tbps



- On 27th November 2016
  - a large number of Deutsche Telekom customers using Speedport home routers reported connectivity problems
  - the root cause of the problem was found to be a new variant of Mirai which was trying to expand the botnet



usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Understanding the Mirai Botnet

Manos Antonakakis, *Georgia Institute of Technology;* Tim April, *Akamai;* Michael Bailey, *University of Illinois, Urbana-Champaign;* Matt Bernhard, *University of Michigan, Ann Arbor;* Elie Bursztein, *Google;* Jaime Cochran, *Cloudflare;* Zakir Durumeric and J. Alex Halderman, *University of Michigan, Ann Arbor;* Luca Invernizzi, *Google;* Michalis Kallitsis, *Merit Network, Inc.;* Deepak Kumar, *University of Illinois, Urbana-Champaign;* Chaz Lever, *Georgia Institute of Technology;* Zane Ma and Joshua Mason, *University of Illinois, Urbana-Champaign;* Damian Menscher, *Google;* Chad Seaman, *Akamai;* Nick Sullivan, *Cloudflare;* Kurt Thomas, *Google;* Yi Zhou, *University of Illinois, Urbana-Champaign*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

This paper is included in the Proceedings of the
26th USENIX Security Symposium
August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

Common trends

- Insecure open ports and default or hard-coded passwords
  - default passwords can be found in pre-compiled dictionaries
  - hard-coded passwords can be found in firmware images
  - initially, Mirai used only 46 default passwords to infect 200 000+ devices
- An increasing number of malware try to exploit software vulnerabilities in IoT devices
  - vulnerabilities may exist in the applications and in the firmware/OS
  - vulnerabilities are used for infection and for privilege escalation
  - some vulnerabilities are exploited just a few weeks after their disclosure
- IoT botnets exhibit a very dynamic behavior
  - rapidly changing malware hosting infrastructure
  - polymorphism (packing)
  - quick evolution (thanks to source code release of some botnets)

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

SETIT = Security Enhancing Technologies for the Internet of Things

- Goal:
  - to 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

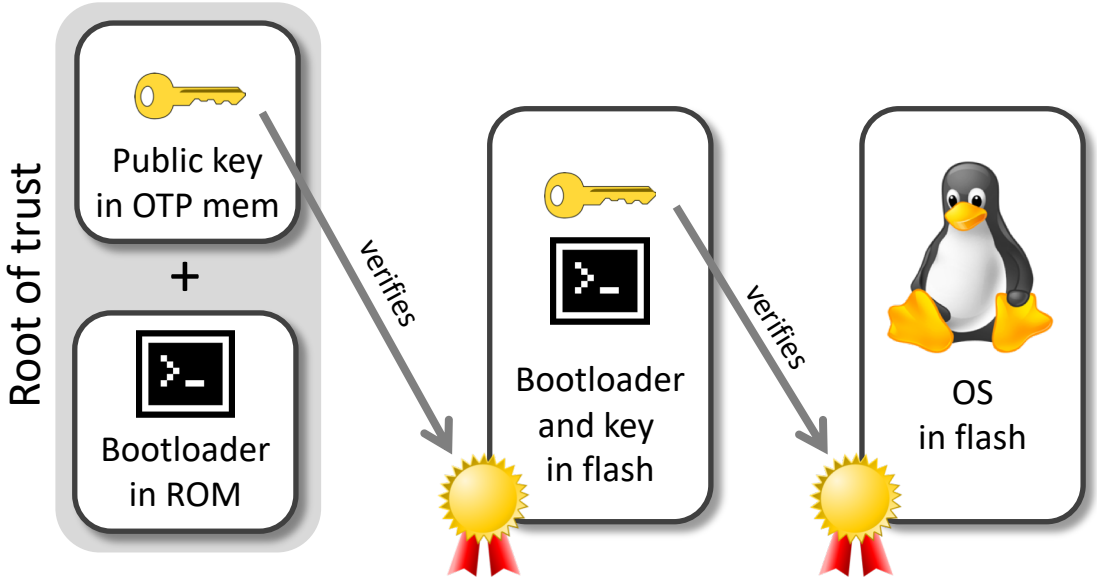
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

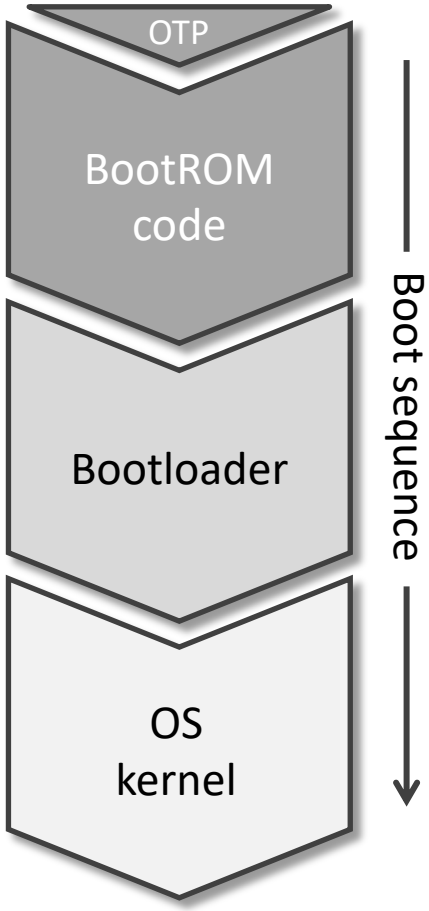
Platform level security for IoT devices

- Research question:
  - Can IoT devices be made more difficult to compromise while still keeping their price low?
- Basic ingredients of a solution:
  - Verified boot
  - Trusted Execution Environment (TEE)
  - 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 and a root of trust
- Implements on a chain of trust

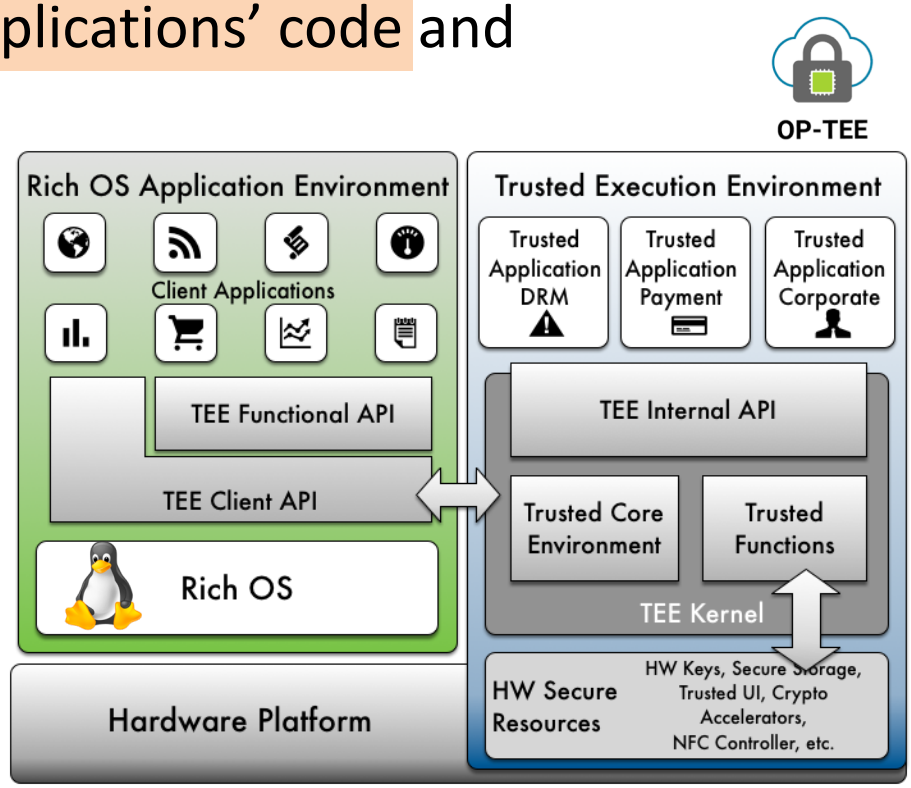




Trusted Execution Environment (TEE)

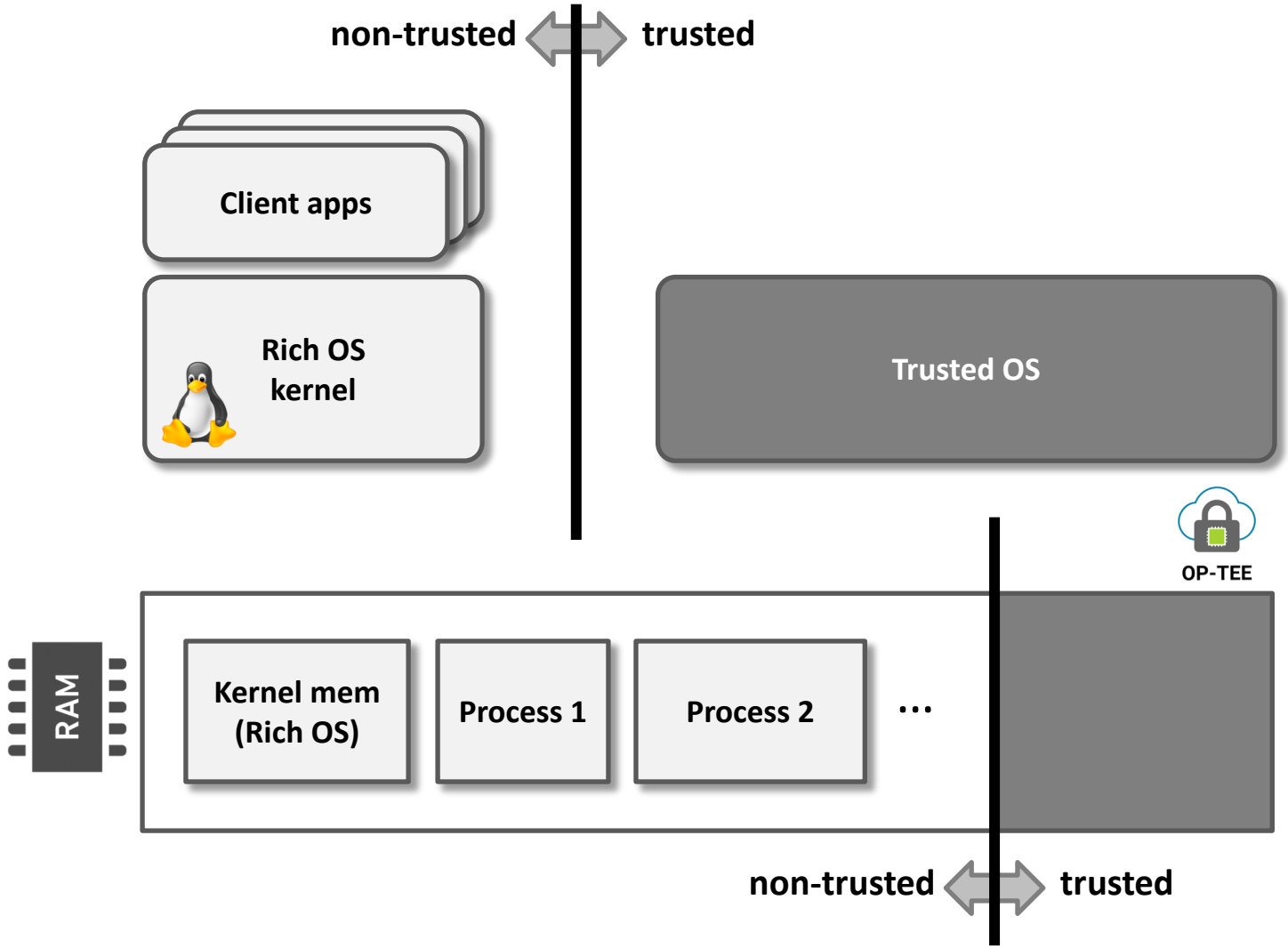
- An isolated execution environment that provides security features such as integrity of applications' code and confidentiality of their data

- Requires hardware support:
  - two security states of the CPU (normal, secure)
  - secure transition to the secure state and back
  - hardware based enforcement of an access control policy to system resources
  - some persistent secure storage available only in secure state

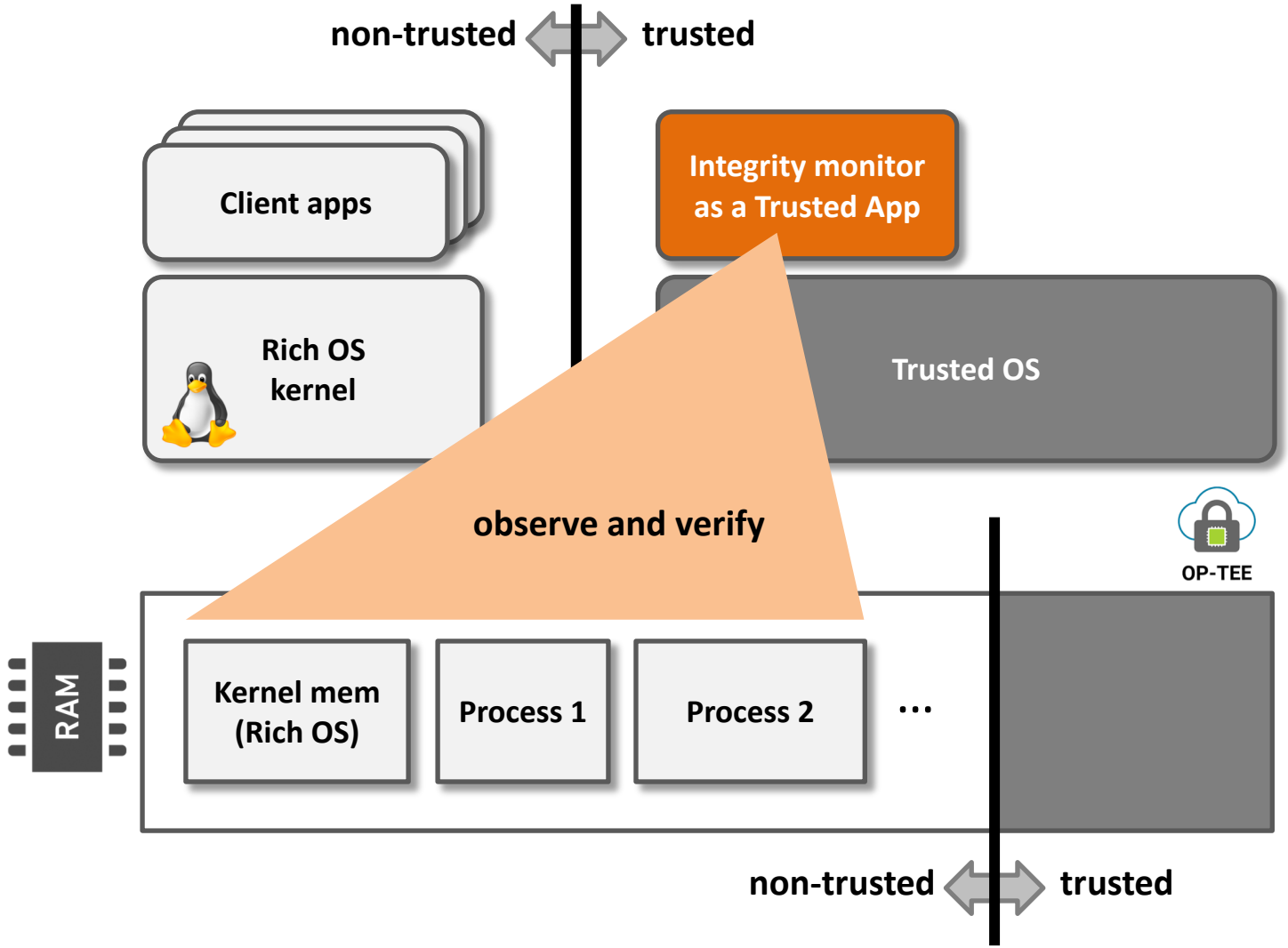


arm TRUSTZONE

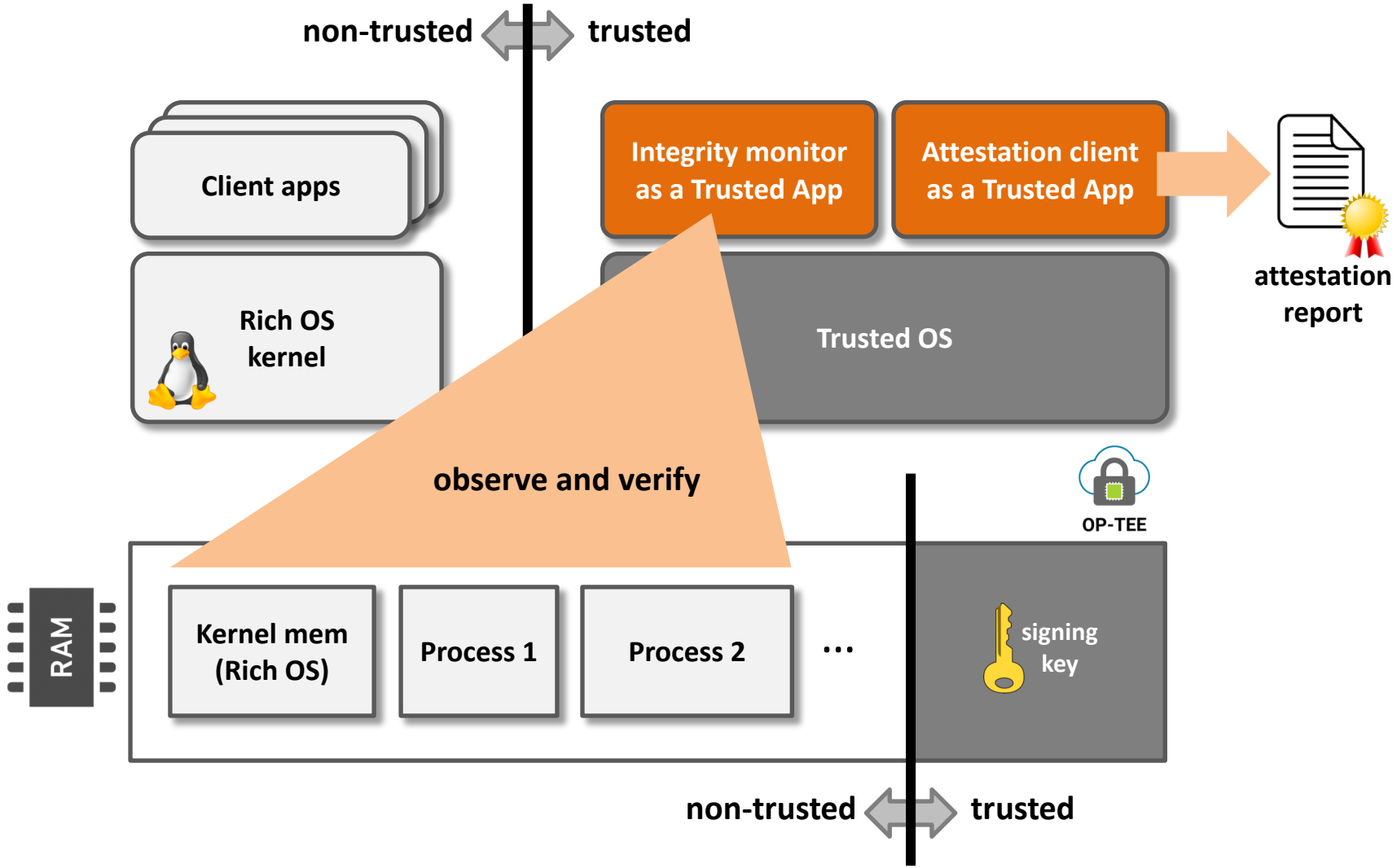
Integrity monitoring and remote attestation



Integrity monitoring and remote attestation

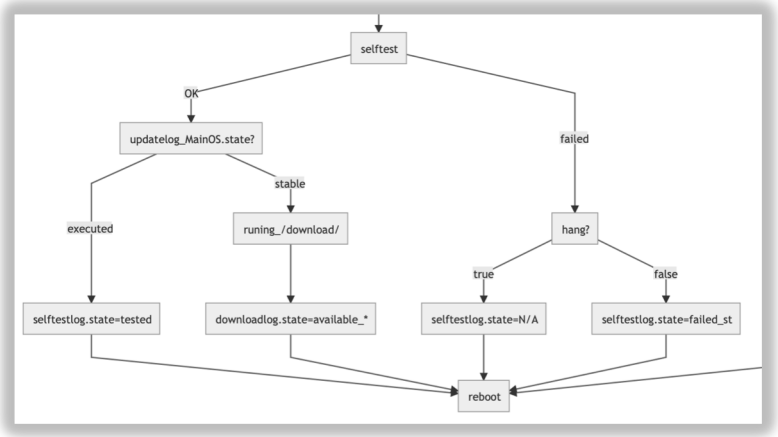


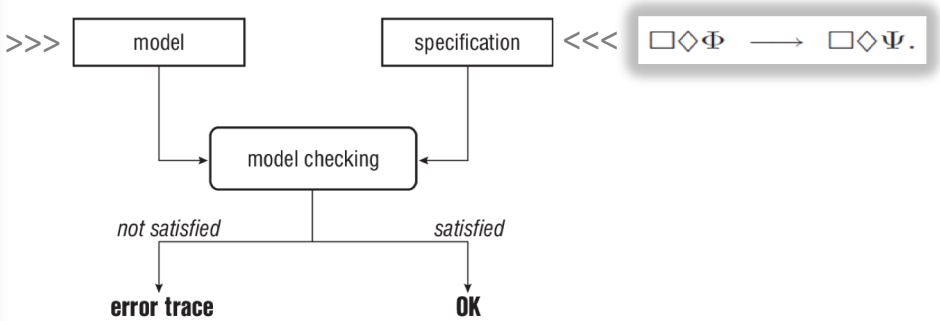
Integrity monitoring and remote attestation



Secure remote software update

- Needed to fix vulnerabilities discovered during device lifetime
- Software updates are downloaded digitally signed
- Update process must ensure
  - fail-safe operation
  - version rollback protection
- We use formal methods to prove these properties





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!

Acknowledgement

This work was supported by the SETIT project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided by the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ INNOVÁCIÓ LENDÜLETE

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Levente Buttyán
buttyan@crysys.hu