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...

THE INTERNET OF THINGS
An Explosion of connected possibility

Billions of devices

Year

1992 1,000,000
2003 0.5 BILLION
2009 IoT INCEPTION
2012 8.7 BILLION
2014 14.4 BILLION
2015 22.9 BILLION
2017 28.4 BILLION
2018 34.8 BILLION
2019 42.1 BILLION
2020 50.1 BILLION

Levente Buttyán
Security Enhancing Technologies for the Internet of Things
IoT applications

Consumer & Home

Smart Infrastructure

Security & Surveillance

Healthcare

Transportation

Retail

Industrial

Others

Vivante and the Vivante logo are trademarks of Vivante Corporation. All other product, image or service names in this presentation are the property of their respective owners. © 2013 Vivante Corporation
How about 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

Hacking Insulin Pumps And Other Medical Devices From Black Hat

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

Internet of Things

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

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

Major DDoS attack knocks Spotify, Twitter, PayPal, and more on Friday

The sound of silence.

Brad Chacos | @BradChacos
Senior Editor, PCWorld

Oct 21, 2016 3:34

Michael Kan
IDG News Service

Oct 21, 2016 4:21 PM
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
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*

---

Diagram:

- **Public key in OTP mem**
- **Bootloader in ROM**
- **Bootloader and key in flash**
- **OS in flash**

Root of trust verifies:

- **Verifies**
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

Client apps

Rich OS kernel

Integrity monitor
as a Trusted App

Attestation client
as a Trusted App

trusted memory

signing key

non-trusted memory

Rich OS kernel

Process 1

Process 2

observe and verify

attestation report
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