Security of IoT Systems

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

- 2020: 50.1 BILLION
- 2019: 42.1 BILLION
- 2018: 34.8 BILLION
- 2017: 28.4 BILLION
- 2016: 22.9 BILLION
- 2015: 18.2 BILLION
- 2014: 14.4 BILLION
- 2012: 8.7 BILLION
- 2009: IoT INCEPTION
- 2003: 0.5 BILLION
- 1992: 1,000,000

"Levente Buttyán
Security of IoT Systems | 2"
Popular IoT applications

- Smart City
- Intelligent Transport
- Connected Car
- Digital Healthcare
- Smart Retail
- Supply Chain Automation
- Precision Agriculture
- Industry 4.0
- Wearables
- Smart Home
How about security?

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

By Nicholas Fearn  February 12, 2017
How about security?

2 Million Home Security Camera Users Give Hackers

Somebody’s Watching: How Home Security Cameras Give Hackers

Ring Home Security

The internet of things

Your Smart

Hacker’s Remotely Kill a Jeep on

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
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

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 = 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
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

---

![Diagram of verified boot process]

1. **Root of trust** in OTP
2. **Bootloader in ROM**
3. **Bootloader and key in flash**
4. **OS in flash**

---

Security of IoT Systems | 14
**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
Integrity monitoring and remote attestation

Client apps

Rich OS
kernel

Trusted OS

Kernel mem
(Rich OS)

Process 1

Process 2

...
Integrity monitoring and remote attestation

- Client apps
- Rich OS kernel
- Integrity monitor as a Trusted App
- Trusted OS
- Kernel mem (Rich OS)
- Process 1
- Process 2
- ...
Integrity monitoring and remote attestation

Client apps
Rich OS kernel

Non-trusted

Integrity monitor as a Trusted App
Attestation client as a Trusted App

Trusted OS

Kernel mem (Rich OS)
Process 1
Process 2
...

Non-trusted

trusted

observe and verify

Attestation report

signing key

OP-TEE

non-trusted

trusted
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.