Security Challenges in the era of Internet-of-Things and Deep Learning

Elena Dubrova
School of Electrical Engineering and Computer Science
Royal Institute of Technology (KTH)
What concerns you about a world of connected IoT devices?

Privacy 62%
Security 54%
Physical safety 27%
Unable to repair 24%
Machines taking over the Earth 21%
Not knowing how to use them 17%
No tangible benefits 11%

Results of a global customer survey (2016) [1]
What defines IoT security?

- Limited resources
- Evolved threat landscape
- New trust models
- Increased privacy concerns

Source:
- https://thenounproject.com/term/handshake/6020
- https://learn.sparkfun.com/tutorials
- http://gizmodo.com/
New trust models

Access and interconnect networks may not be trustworthy
- Access network may be operated by a shopping mall, a coffee shop, etc.
- 3rd parties may access to interconnect network, e.g., for analysis

Intermediaries on which IoT systems rely may not be trustworthy
- IoT devices which mostly sleep rely on proxies to cache requests and responses
- In mesh networks, every node is an intermediary
Increased privacy concerns

• Big data generated in IoT opens great opportunities for analytics, automation, and process and resource optimization
• But it also increases the risk of privacy breaches

Secret surveillance of Norway’s leaders detected

Hacker looks to sell 9.3 million alleged patient healthcare records on the dark web

By James Rogers
Published June 29, 2016
FoxNews.com
Evolved threat landscape

- Increased **attack surface**
- Increased **value** for attackers
- Decreased **cost** of performing attacks
- Increased **damage** when attack happen
Limited resources

- IoT devices with limited **computing, storage, and communication** resources may not be able to afford standard cryptographic algorithms and protocols
- Battery-operated IoT devices need to be **energy** efficient to prolong their lifetime
- Ensuring robust over-the-air firmware and software **updates** is crucial, but challenging when:
  - there is not enough memory to save both old and new updates
  - applications are infected by viruses blocking the updates
How to assure IoT devices?

Energy-Efficient Crypto

Tamper Resistance

Supply Chain Security

source: https://www.emnify.com/2016/08/17/iot-security-sms/
Assuring Tamper Resistance
Why tampering?

- Theft of service
  - Getting a service for free
    - pay-TV, parking cards, electricity meters, …
- Denial of service
  - Dishonest competition
- Theft of Intellectual Property (IP)
  - Reverse engineering/cloning/counterfeiting for marketplace advantage
- Theft of sensitive data/personal information
  - Steal the secret key
How to tamper?

• Invasively intrude a chip/board

• **Measure side-channel signals, e.g.**
  power consumption, EM emissions, timing

• Inject faults to corrupt the computation and exploit the effect

source: sec.ei.tum.de

source: hackaday.com
Traditional key storage methods

• Fuses
• Non-volatile memories (Flash, EEPROM, …)
• Volatile memories (SRAM) with a battery

• Problem with memory-based storage
  • Residuals of data may remain after erasure
    – data remanence
Data remanence in volatile memories

Volatile memories (SRAM, DRAM) do not entirely lose their contents when power is turned off

- for SRAM, at room temperature the data retention time varies from 0.1 to 10 sec
- cooling SRAM to -20ºC increases the retention time to 1 sec to 17 min
- at -50ºC the retention time is 10 sec to 10 hours

“Physical Attacks on Tamper Resistance: Progress and Lessons”, S. Skorobogatov, Special Workshop on HW Assurance, 2011
Novel key storage method: Physical Unclonable Functions (PUFs)

- Due to manufacturing process variations, every chip is slightly different
- We can use these differences to create a unique “fingerprint” for each chip
Arbiter PUF

Creates a race between two identical paths
  – process variations cause small differences in delays
Advantages of PUF-based key storage

<table>
<thead>
<tr>
<th></th>
<th>PUF</th>
<th>TRNG + Memory</th>
<th>External Key Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Generated on-chip</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>No Secure Storage Needed</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Key Invisible at Power Off</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
PUF research at KTH

We design PUFs which are among the best in the state-of-the-art in terms of energy efficiency and reliability

“Temperature Aware Phase/Frequency Detector-Based RO-PUFs Exploiting Bulk-Controlled Oscillators”, S. Tao, E. Dubrova, DATE’2017, March 27-31
Side-channel attacks

• Side-channel signals are related to the data processed
  • e.g. different amount of power is consumed

• Do not require expensive equipment

• Deep Learning (DL) makes possible a new type of side-channel attacks

source: hackaday.com
Side-channel attacks before and after DL

Before DL

After DL

source: riscure.com
DL-based side-channel attack - Profiling stage

1. Apply random plaintext & keys

2. Create training/validation labeled data sets

3. Train neural network

source: risecure.com

Leakage model
DL-based side-channel attack – Attack stage

1. Apply random plaintext
2. Capture power trace
3. Classify key candidates

source: riscure.com
Side-channel attack research at KTH

- Attack on USIM card using power consumption
- Attack on a Bluetooth device using EM far filed emissions
- Attack on a protected arbiter PUF implemented in FPGA using power consumption combined with bitstream modification
The secret key can be extracted from USIM using 4 power traces on average (20 in the worst case) [3]
The AES encryption key can be extracted from a Bluetooth device (Nordic Semiconductor nRF52 DK) from 10K EM traces captured at 15 m distance [4]
Responses of a protected arbiter PUF can be extracted from its FPGA implementation (Xilinux 28 nm Artix 7) using power traces [5]
Summary and future work

• **Needs** for tamper-resistance of IoT devices grow due to
  • physical accessibility
  • increased value of stored/processed information

• **Difficulty** to assure tamper-resistance also grows due to
  • constrained resources
  • recent progress in physical attacks
  • lack of protection

• We need to understand possibilities and limitations of physical attacks making use of DL and develop defenses
References


