Hardware & IoT Security

Mustakimur R. Khandaker

Why?

Modern security work is largely focused on either protecting or attacking target operating systems.

- Software is not enough to fully protect a system.

Security in hardware offers performance and power consumption advantages over its software equivalents.

- Increasing amounts of data being processed and the complexity of encryption algorithms slows down security implementations severely.
- Often times these same encryption algorithms can be implemented in hardware.
  - e.g. Intel AES-NI.

Hardware Features

Trusted Platform Module (TPM).
- Measure and attest the software running on a computer.

ARM TrustZone.
- Restrict execution of compromised operating systems.

Intel Software Guard Extensions (SGX).
- Protect processing from compromised operating systems.

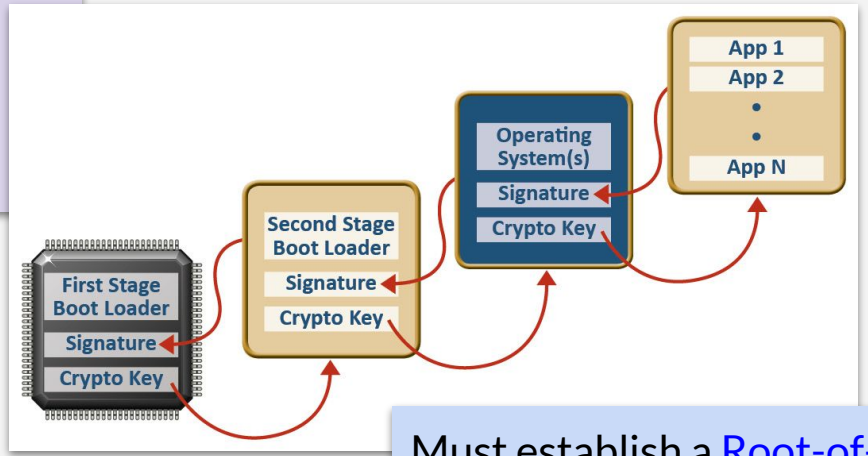
Intel Processor Trace (IPT).
- Track control flow events.

Intel Memory Protection Extensions (MPX).
- Check and enforce memory bounds.

Secure Boot

Check each stage in the boot process.

- Is code that you are going to load acceptable?
- If not, terminate the boot process.



Must establish a Root-of-Trust.

- A component trusted to speak for the correctness of others.
- Assumed to be correct because errors are undetectable.

Side Channel Attack

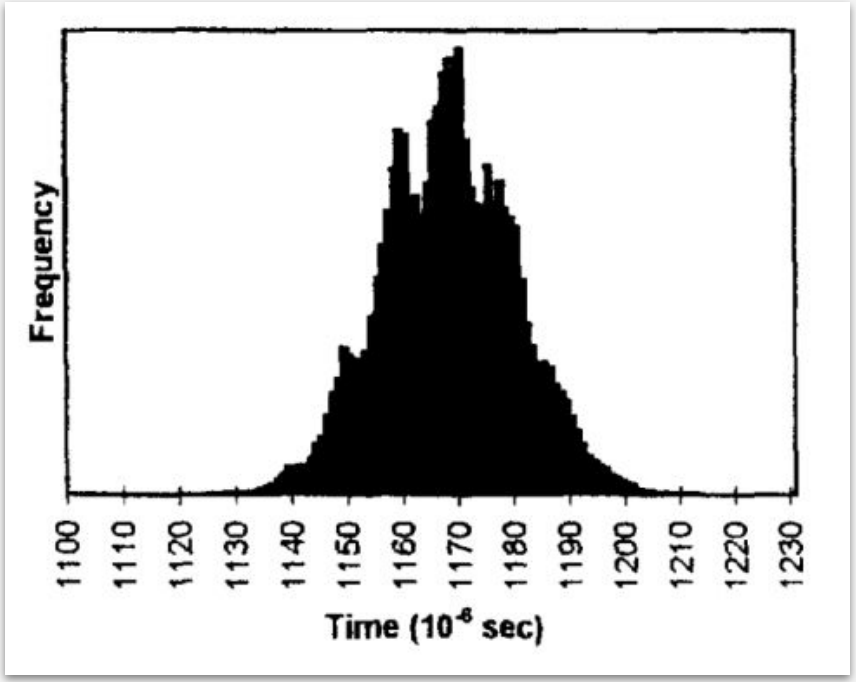
In cryptography, a side-channel attack is an attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis).

Type of side channel:

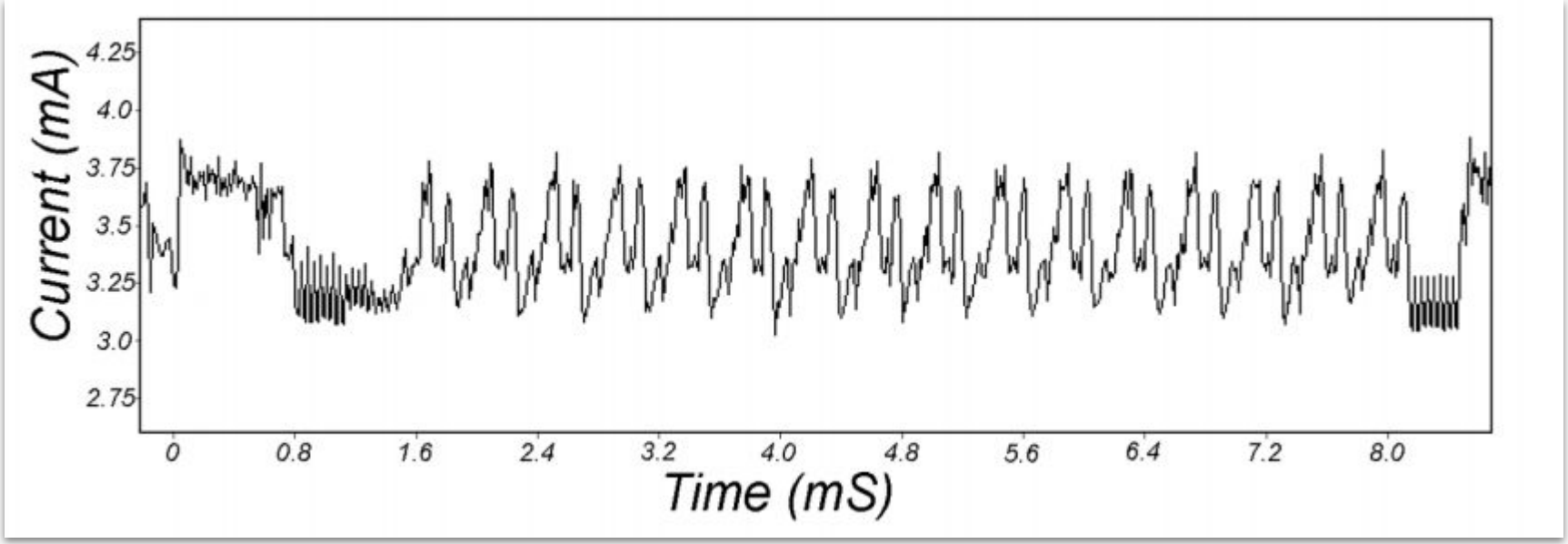
- Timing channel.
- Power channel.
- EM radiation channel.
- Acoustic channel.
- Photonic emission channel.

Timing Side Channel

- The execution time of e.g. RSA depends on the value of secret data/key.
- By timing the execution for a particular public input, one obtains information about the secret.
- By adaptively modifying the public input and measuring the execution times one can uncover the key bit by bit.



Power Channel



The power consumption of a chip depends on the secret data that is used in the computation on the chip. One is able to uncover the secret data by measuring the power consumption of the entire chip.

Cache Side Channel

Data present in caches can be accessed faster than from memory.

- For multilevel caches, data accessed from **L1 cache** has lower latency than from an **L2 cache**.

The cache interference and time difference for the access patterns leaks information:

- Certain memory contents exist in cache or not.
- Shows that data has been accessed recently.

This attack is useful to find keys for encryption process.

Meltdown

Meltdown allows attackers to read arbitrary physical memory (including kernel memory) from an unprivileged user process.

Meltdown uses **out of order instruction execution** to leak data via a processor covert channel (cache lines).

Meltdown was patched (in Linux) with KAISER/KPTI.

Speculative Execution

Modern processors perform speculative execution.

They **execute instructions in parallel** that are likely to be executed after a branch in code (e.g. if/else).

Of course these instructions may never really be executed, so a sort of CPU snapshot is taken at the branch so **execution can be "rolled back" if needed**.

How does the CPU know which side of a branch ("if/else") to speculatively execute?

- Branch prediction algorithms **are trained** based on current execution.
- The CPU "learns" which branch will be executed from previous executions of the same code.

Spectre

Spectre abuses **branch prediction and speculative execution** to leak data from via a processor covert channel (cache lines).

Spectre can only read memory from the current process, not the kernel and other physical memory.

Spectre does not appear to be patched.

IoT Security

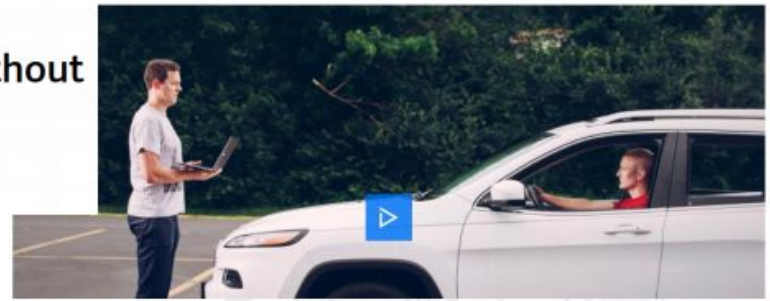
- Understand threats and assets.
- Consider context of use.
- Highlight security good practices in specific sectors.
- Provide recommendations to enhance cyber security.
- Expert groups.

Threats

by Tom Spring August 11, 2016 , 11:27 am

by Tom Spring August 26, 2016 , 2:55 pm

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



circuit breaker

This doll recorded kids' conversations without parental consent

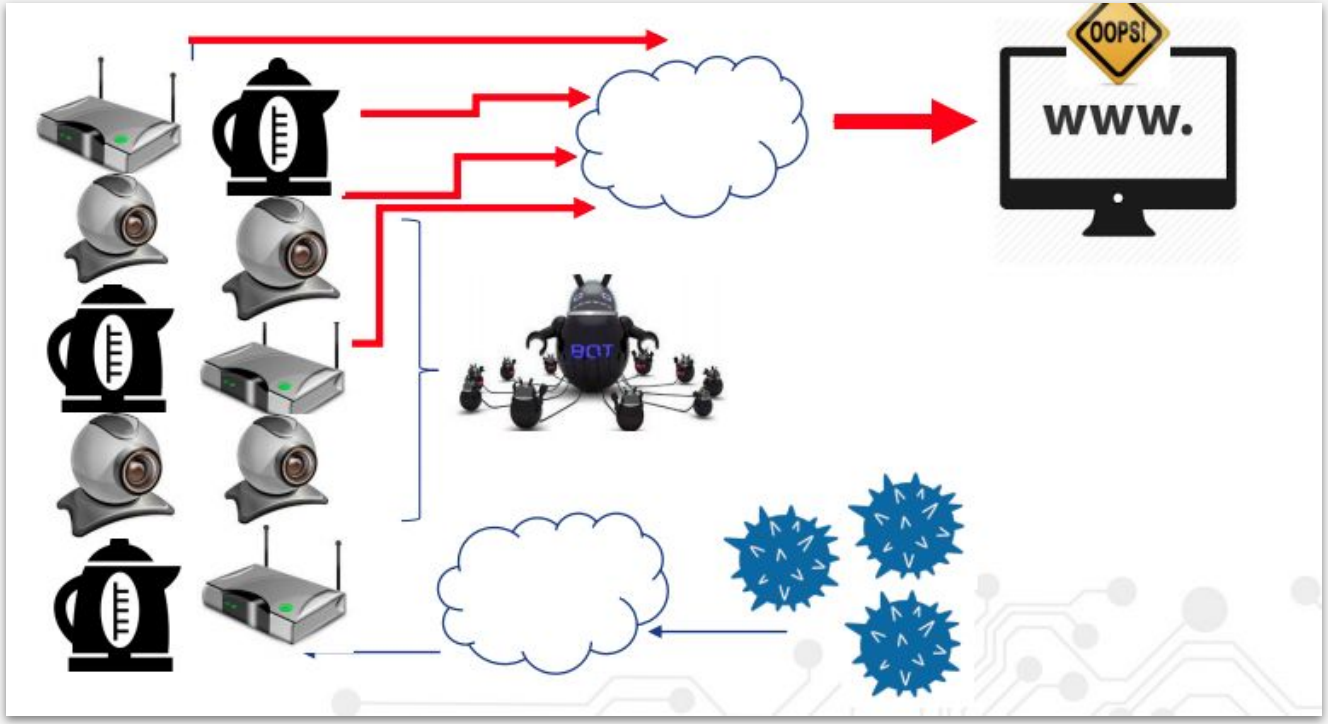
Security experts found ways to listen in

by Ashley Carman | @ashleyrcarman | Dec 8, 2016, 11:36am EST

DDoS Attack

IoT botnet:

- IoT devices used for DDoS attacks.



Challenges

- Very large attack surface and widespread deployment.
- Limited device resources.
- Lack of standards and regulations.
- Safety and security process integration.
- Security by design not a top priority.
- Lack of expertise.
- Applying security updates.
- Insecure development.
- Unclear liabilities.

< Hardware and IoT Security />