Side Channel Attacks

COM-402: Information Security and Privacy

(slide credits: Nicolas Gailly)
Side Channel: Why bother?

- Many fast growing fields for embedded applications: RFID, sensor networks, “Internet of Things”
- Areas of interest: public transportation, communication, health care, car industry, banking sector, military, etc.
- Drastic increase in the importance of hardware security and the demand for secure chips
- Hardware implementing cryptographic functions (including smartcards) often show severe vulnerabilities

https://zerabyteio/talks/2013-01-28-ieeepdf
Side Channel: Definition

Before side channel cryptanalysis, a cryptographic system was only conceived as:

![Diagram showing the relationship between Input, System, and Output](image-url)
Side Channel: Definition

- Starting mid-90s, a new broader definition
- Attacks target the system device itself without relying on input/output pair
Examples of Side Channels

- How much power the computer uses when it does something
- How long it takes the computer to do something
- Which areas of the computer’s memory have been accessed
- Unintentional electromagnetic radiation emanating from the system
- Sounds coming from the system (beeps, hard drives working, etc.)
- The time that network packets get sent out of the system
Side Channel: Timing Attacks

- Cryptosystems take slightly different amounts of time depending on the input data (i.e., secret key)
- Feed the timing measurements to a statistical model
- Model can guess key with some degree of certainty
- Attack is non-invasive and passive

- RSA: Square and multiply algorithm:
  - If the \(i^{\text{th}}\) bit of secret key is 1, do a modular reduction
  - If the \(i^{\text{th}}\) bit of secret key is 0, continue to next bit
- Time difference is enough to guess the \(i^{\text{th}}\) bit

\[
x = C \\
\text{for } j = 1 \text{ to } n \\
\quad x = \text{mod}(x^2, N) \\
\quad \text{if } d_j == 1 \text{ then} \\
\quad \quad x = \text{mod}(xC, N) \\
\quad \text{end if} \\
\text{next } j \\
\text{return } x
\]
Timing Attack: SSH Keystrokes

- SSH (interactive) sends one packet for each key pressed
- Infer key typed by correlation with timing information!

Figure 1: The traffic signature associated with running SU in a SSH session. The numbers in the figure are the size (in bytes) of the corresponding packet payloads.

https://people.eecs.berkeley.edu/~daw/papers/ssh-use01.pdf
Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in the cache
- Assumptions: AES and attacker share the same CPU
  (assumption can be relaxed)

https://cryptojediorg/peter/data/croatia-20160610pdf
Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in cache
- AES and attacker share the same CPU
  - Attacker **evicts** some entries

https://cryptojediorg/peter/data/croatia-20160610pdf
Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in cache
- AES and attacker share the same CPU
- Attacker **evicts** some entries
- AES **loads** the data from table

https://cryptojediorg/peter/data/croatia-20160610pdf
Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in cache
- AES and attacker share the same CPU
- Attacker **evicts** some entries
- AES **loads** the data from table
- Attacker **loads** same entry
  - Fast lookup → AES did **not** load from this line
  - Slow → AES loaded from this line
- **Leaks** secret key bits!

https://cryptojediorg/peter/data/croatia-20160610pdf
Timing Attacks: Flush + Reload

- Extract RSA private key from cache access timing information
- Attacker process flushes the cache, waits, then loads same information
- Time to fetch from the cache depends on the victim process’s activity
- Works even on different VMs on same host!

https://eprintiacrorg/2013/448pdf
Timing Attacks: Defenses

- General data-independent calculations:
  - Same time for any computations
  - Or at least same number of clock cycle if computation done using input data

- Avoid conditional branch and secret intermediates
  - Using XOR, OR etc operations instead of IF / ELSE
  - Takes the same amount of time *and* power

- Introduce random delays of a few milliseconds
  - Closes fine-grained but not coarse-grained timing channels

- Most of the time reasonable defenses are available if used properly!
Side Channel: Power Analysis Attacks

- Every circuit with transistors consume power (smartcards, mobile phone, etc.)
- Monitoring the power consumption reveals informations stored in the circuit
- The attack is cheap and non-invasive (USB sound card, some wires and a probe)
- Very successful in practice: Can recover ECDSA private key during signature

https://wwwtauacil/~tromer/handsoff/
Side Channel: Simple Power Analysis

- Often requires detailed knowledge about device + implementation
- Triple-DES power analysis reveal key easily

http://wwwnicolas courtoiscom/papers/sc/sidech attackspdf
Side Channel: Simpler Power Analysis RSA

- RSA uses **Square-and-Multiply**:
  - Loop over each bits of the secret key
  - If bit is 1 => multiply then square => more power consumption
  - If bit is 0 => square directly

- Leaks the secret key entirely!

```
x = C
for j = 1 to n
x = mod(x^2, N)
if d_j == 1 then
x = mod(xC, N)
end if
next j
return x
```

http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks
Side Channel: Differential Power Analysis

- Use of advanced statistical techniques including error correction, noise filtering methods, etc.

- General technique:
  - Observe $m$ encryption operations: ciphertext and power traces
  - Choose a selection function $S$: it’s a guess over the key $K$
  - Run $k$ sample differential traces
  - If the guess is good, it will show
Power reference

Correct $K_s$

Incorrect $K_s$

1000 samples

http://gaussececsucedu/Courses/c653/lectures/SideC/lecture11-dpapdf
Side Channel: Differential Power Analysis

- DPA can be used to break any algorithm in principle
- DPA can also be used to reverse engineer closed-source protocols

**Defenses:**
- Reduce signal size
- Introduce noise
- Design cryptosystems with realistic assumptions about the underlying hardware
Side Channel: Electromagnetics

- Electromagnetic signal measured with a magnetic probe + digital card: works **through a wall**
- Detect DOUBLE and ADD operations of ECDSA signatures
- Much harder than RSA because much faster (more advanced signal processing techniques)

![Image of electromagnetic signal measurement](https://www.cstau.ac.il/~tromer/mobilesc/)

A segment of the electromagnetic signal, after singular spectrum analysis.
Electromagnetics: A Long History Reality

- Every electrical device generates magnetic radiations:
  - Screens, laptops, mobiles, etc.
- Exploited by NSA TEMPEST program since 1943!
- First public knowledge in 1972

https://www.wired.com/2008/04/nsa-releases-se/
https://climateviewer.com/
Side Channel: Electromagnetics

- Attack possible with consumer grade radio receiver or even with handmade receiver!

https://wwwcstauacil/~tromer/radioexp/
Side Channel: Acoustic Cryptanalysis

- Recover information from acoustic sounds of the voltage regulator inside the PC (“whining” sound)
  - Goal: recovery of a 4096-bit private key used in RSA encryption
  - Requires at least 2048 decryptions, bit-by-bit key recovery
  - Attack vector: Enigmail with Thunderbird GPG plugin, automatic decryption when receiving email

https://www.slideshare.net/dusanklinec1/accoustic-crypto-33236263?from_action=save
Acoustic Cryptanalysis
Acoustic Cryptanalysis: RSA - CRT

Textbook RSA encryption:
\[ c = m^e \mod n \]
- \( m \): message
- \( e \): public key exponent
- \( n \): public key modulus \( n = p \times q \)

Textbook RSA decryption:
\[ m = c^d \mod n \]
- \( m \): message
- \( d \): private key exponent
- \( n \): public key modulus \( n = p \times q \)

Chinese Remainder Theorem (CRT) optimization:

**Precompute:**
- \( d_p = d \mod p-1 \)
- \( d_q = d \mod q-1 \)
- \( q_{\text{inv}} = q^{-1} \mod p \)

**Decryption:**
\[ m1 = c^{(d_p)} \mod p \]
\[ m2 = c^{(d_q)} \mod q \]
\[ h = q_{\text{inv}} \times (m1 - m2) \mod p \]
\[ m = m2 + h \times q \]
Acoustic Cryptanalysis: RSA

- General algorithm:
  - Guess $i^{th}$ bit of the key → 1 or 0
  - Submit to decryption (decryption oracle)
  - Observe difference between the mod $p$ and mod $q$ operations

(a) attacking 0 bit
(b) attacking 1 bit
Side Channel: Fault Attacks

- **Inject** faults into the system
  - Change voltage, tamper the clock, etc.
- Smartcard hacking is a huge business
  - Paid TV content
  - ATMs
  - Laundry machines!!

The FBI Warns of Hackers Who Get ATMs to Spit Out Millions in Cash

http://inforippleshotcom/blog/the-brief-history-of-chip-card-hacking
Side Channel: Differential Fault Analysis

- **Inject** faults into the system
  - Change voltage, tamper the clock, etc.
- Encrypt data twice and compare results
  - One bit difference indicates a fault in one operation
- Able to attack RSA, DES, etc.

```
(1) Plaintext
    Cryptographic Implementation
    Non-faulty Ciphertext

(2) Plaintext
    Cryptographic Implementation
    Faulty Ciphertext

(3) Analysis
```

Fault Injection
RowHammer

- Memory access rapidly activating same memory rows
- Accesses modify contents of nearby memory rows
- Attack can:
  - Gain root access
  - Escape sand boxes
  - Make apps with higher privileges, etc.
Side Channel: Optical Covert Channel

- Exfiltrate data from air-gapped computers
- Data exfiltration through the drive LEDs’ blink frequency
- LED blinks encode a QR-code encoded data
- Analyzed by remote camera (e.g., mounted on drone!)

[Diagram of data exfiltration process]

Conclusion

● Side-channel risks come in many shapes and sizes
  ○ Timing, power, visual, acoustic, faults, …
  ○ Can be exploited to exfiltrate secrets, fingerprint systems or users, …

● Important to develop defensively with awareness of side-channel risks
  ○ Example: constant-time implementations of code handling sensitive secrets
  ○ No all-purpose, general defense exists (yet), unfortunately