Emission Security and Side-channel Attacks

By Andrey Leshenko

Comp Sec Seminar 2017 (With Orr Dunkelman)
“...I was at home, sleeping...”
The Polygraph

What a polygraph measures:
- Body movements
- Breathing (diaphragm)
- Breathing (chest)
- Perspiration
- Pulse, blood pressure

1. Blood pressure cuff records pulse, blood pressure
2. Rubber tubes placed over chest and abdomen record breathing
3. Two metal plates attached to fingers record sweating

Laptop connects to polygraph
A Side-channel Attack

- Any attack based on information gained from the physical implementation of a cryptosystem.
"PASSWORD INCORRECT"
TIME CHANNEL
Comparing Secret Keys

char *key = “SECRET”;
char *input = get_input();

memcmp(key, input, KEY_LEN)
likely implementation (simplified)

```c
int memcmp(char *a, char *b, int len)
{
    for (int i = 0; i < len; i++) {
        if (a[i] != b[i])
            return 1;
    }

    return 0;
}
```
Guessing the First Byte

Time

"MAA" "NAA" "OAA" "PAA" "QAA" "RAA" "SAA" "TAA" "UAA" "VAA"
Timing Attacks

1. Timing depends on secret data
2. Attacker measures timing
3. Attacker recovers secret data
int CRYPTO_memcmp(char *a, char *b, int len) {
    char bit_diff = 0;

    for (int i = 0; i < len; i++) {
        bit_diff |= a[i] ^ b[i];
    }

    return bit_diff;
}
Examples

- 2006: Recover **AES-256** secret key of Linux’s dmcrypt in just 65 ms (Osvik, Shamir, Tromer)
- 2013: “Lucky13” recovers plaintext of CBC-mode encryption in most **TLS** implementations (AlFardan, Paterson)
- 2014: Attack against **RSA-2048** in GnuPG 1.4.13: “On average, the attack is able to recover 96.7% of the bits of the secret key by observing a single signature or decryption round.” (Yarom, Falkner)
Further Complications

- Compiler optimizations
- Time dependence of multiplication
- Code branching
- Cache misses and page faults
ELECTRO MAGNETIC EMISSIONS CHANNEL
Magnetic field from electric current
A Small Demo
World War I
Van Eck Phreaking

• 1985: Win van Eck showed the picture on a computer monitor could be reconstructed from EM emissions

Figure 4.3: Text signal received from a 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls).

https://i.stack.imgur.com/7Bxqb.png
Software Protection

- Most of the emissions are from the high frequencies
- Ross Anderson, Markus Kuhn, filter them using software methods

Ross Anderson, Security Engineering
Voting Machines

TEMPEST

• Codename for EM emission based attack and defense

• Protection standards exist:
  – Shielding
  – RED/BLACK separation
  – Distance of equipment from walls and pipes

• Hardware complying with these standards exists, but it very expensive
POWER CONSUMPTION CHANNEL
Smartcards

- A small chip
- Power is externally supplied
- Often contains secret keys
Power Analysis

Power usage of RSA algorithm


http://m.eet.com/media/1180271/f2xl.jpg
Differential Power Analysis

- (Paul Kocher, 1998)
- If an attacker collects many samples of encryptions using a known plaintext,
- He can use statistical methods to test hypotheses about the key,
- Resulting in a very robust attack
Solutions

• Adding randomness to the protocols
• Adding randomness to the computations
• Processors that add dummy operations and change clock speed every few cycles
AUDIO CHANNEL
Keyboard Noises

• Typed text can be reconstructed from an audio recording (2004, Asonov and Agrawal. 2005, Zhuang, Zhou, and Tygar)
Acoustic Crypto-analysis

- Electric current causes vibrations
Acoustic Crypto-analysis

- 2004, Eran Tromer and Adi Shamir

Cross-device Tracking

• Audio beacons can be embedded in TV ads or placed in stores
• Mobile apps can then listen, and track the user and his habits
• The field is still developing as of 2017. *SilverPush* is a major player.
VISIBLE LIGHT CHANNEL
Informative LEDs

- Joe Loughry and David Umphress
Monitor Illumination

• 2002 Markus Kuhn
Results

- 2002 Markus Kuhn

Displayed image

https://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf

Light sensor output

After some processing
"PASSWORD INCORRECT"

EM CHANNEL

INPUT/OUTPUT

TIME CHANNEL

POWER USAGE CHANNEL

LIGHT CHANNEL

AUDIO CHANNEL

???

??

????
Conclusions

• Computer are physical machines. Be aware of the different channels
• Deny physical access when possible
• Use battle-tested crypto libs
• Shielded hardware and buildings may sometimes be the solution
Questions?
THE END
Sources

- Ross Anderson, Security Engineering
- Original papers which presented the attacks
- Graphics sources are written in the presentation notes
- [http://www.edn.com/Home/PrintView?contentItemId=4410267](http://www.edn.com/Home/PrintView?contentItemId=4410267)
- [https://en.wikipedia.org/wiki/Van_Eck_phreaking](https://en.wikipedia.org/wiki/Van_Eck_phreaking)