Everything Can Be Hacked

D. Gritzalis, G. Iakovakis, S. Giannitsari, S. Vasilellis
May 2016
Everything Can Be Hacked. Yes. Everything.

2nd ICT Security World Congress
Athens, May 2016
Incidents of not everyday attacks

Operation Aurora
Targeting the Power Grid

Implantable Medical Devices
An attacker can kill you. Really.

Laser printer
Data sent to printer and ...leaked!

RSA
The Holy Grail of the commercial world’s cryptosystems? Not any more.
Operation Aurora
Targeting the Power Grid

CNN video of the Aurora attack, September 2007,
https://muckrock.s3.amazonaws.com/foia_files/aurora_high_res.wmv
CNN, How hackers can kill you, June 2013, Source: https://www.youtube.com/watch?v=j99FpciyzSQ
Operation Aurora: Targeting the Power Grid

Aurora experiment

- A computer program rapidly opens/closes a 2.25MW, 27 ton diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode
- **Means:** Malicious use of a protective relay or other digital protection
- **Impact:** Control device inflicts an out-of-sync condition
- **Result:** Physical damage to rotational equipment

Timeline

Mar 4, 2007: US Dept. of Energy, Idaho Laboratory (test area)
Jun 21, 2007: NERC (North American Electric Reliability Corp.) notified industry about the Aurora vulnerability
Sep 27, 2007: CNN released a previously-classified demonstration video of the Aurora attack
Jul 3, 2014: US Dept. of Homeland Security released data related to Aurora as part of a FOIA (Freedom of Information Act) request
A simplified Control Diagram

The abrupt opening and closing of the protective circuit changes the behavior of the relay from providing maximum protection to inflicting maximum damage.
Implantable Medical Devices
An attacker can kill you. Really.


Hacking Implantable Medical Devices

Implantable Medical Devices (IMD)
Wireless implantable medical devices, such as Cardiac Pacemakers, Defibrillators, Cochlear Implants, Neuro-stimulators, Insulin Pumps, etc.

Users
• 300,000 Americans per year receive IMD
• There exist >300 such devices, built by >40 manufacturers
• 2.5 million people in US rely on IMD to treat a variety of illnesses

Alert
US Dept. of Homeland Security issued an alert, warning medical facilities for vulnerabilities which could be exploited by an attacker

Vulnerability
• Hacker Barnaby Jack demonstrated how he could compromise an insulin pump from 90m using the high-gain antenna (2011)
• His testimony led the US Food And Drug Administration to change regulations regarding wireless medical devices (2012)
IMD and ICD communication with a programmer

**IMD**: Implantable Medical Devices
**ICD**: Implantable Cardiac Defibrillator
Laser printer
Data sent to printer and ...leaked!


Laser Printer Data Leakage

**Compromising Emanations (CE)**
- Electrical or acoustical energy unintentionally emitted by many sources within equipment/systems that process information
- May relate to the original message or the information being processed
- Can lead to recovery of the plaintext

**Emission investigation of a laser printer**
- Electromagnetic Radiation (ER), Power Line Conductors (PLC), Signal Line Conductors (SLC)

**Analysis of Compromised Emanations**
- Examination of candidate frequency points in the frequency domain
- AM-demodulation of emitted signal with proper bandwidth
  - Identify data-related emanation with spectrum analyzer
- Sampling of these frequency points with storage oscilloscope
  - Decide if relation is a compromising emanation or not
- Conversion of collected data to 2D image
  - Signal and image processing techniques

**Result**
Vulnerability of commercial laser printers in a noisy environment
Measurement setup and initial experimental results
RSA

The Holy Grail of the commercial world’s cryptosystems? Not anymore.

RSA Key extraction via low-bandwidth Acoustic Cryptanalysis

• **RSA** is a **public-key encryption cryptosystem**, widely used for **securing sensitive data**, particularly when being sent **over insecure network**

• During computer operations high-pitched **noises are diffused** due to **vibration of electronic components**

• These produced noises can **leak** information about the **running software** and **sensitive information of security computations**, such as **RSA cryptosystem**

• It was proven that RSA **creates different sounds for every key generation** but individual key bits were not clear due to low bandwidth acoustic channel
RSA key extraction via low-bandwidth Acoustic Cryptanalysis – The attack

Acoustic Cryptanalysis key extraction attack can extract full 4096-bit RSA keys.

Various models of laptops were attacked. Key was decrypted within 1 hour.

Various experiments were executed:
- Using plain mobile phones
- Employing sensitive microphones

Low-bandwidth attack can be performed by measuring the electric potential of a computer chassis. Therefore, an attacker can gain the required leakage of information just by touching the computer or from the ground wires, such as Ethernet, USB, etc.
RSA key extraction via low-bandwidth
Acoustic Cryptanalysis – Methodology

The **mobile phone** attack was performed using a **regular** phone, placed 30cm away of the targeted laptop.

The **sensitive phone** attack was performed by placing:

- A *parabolic* sensitive microphone 4m away
- A *simple* sensitive microphone 1m away
To human ears the resulted leakage sounds like high-pitched noise.

To make this audible one can select the interesting frequencies using a band pass filter and downshift them to within human hearing range.

In recording several pairs of tones can be discerned:
- Each such pair is the sound made by a single RSA decryption.

The key extraction finds secret key bits, one-by-one, sequentially.

For each bit, the attacker crafts a cipher text of a special form:
- The attacker then triggers decryption of chosen cipher text.
- Records the resulting sound.
- Analyzes this sound.

![Attacking the bit 0](image1.png) ![Attacking the bit 1](image2.png)
Everything Can Be Hacked.
Yes. Everything.
One Way or Another.
Sooner or Later.
By Those With a Motive.
References

2. CNN, How hackers can kill you, June 2013, Source: https://www.youtube.com/watch?v=j99FpceiyzSQ