

Emission Security

Nadav Krasnopolsky

based on chapter 17 of Ross Andresson's book "Security Engineering"

Introduction

- Most electronic devices emit electromagnetic radiation (not intentionally).
- This radiation can be used by an opponent to gain privileged information, or disrupt the functionality of the device.
- An opponent could also use other signals coming in or out of an electronic device (such as power or clock cycles).
- All these are referred to as emanations.

Introduction cont.

- Attacks that use emanations are called Emission Attacks, or Side Channel attacks.
- Emission Security (Emsec) - preventing attacks using compromising emanations.

Motivation

Military - stray RF emitted by computers and other electronic equipment could be picked up by an opponent.

Electronic Voting - an attacker could acquire the data (votes) from distance.

Smartcard - can be broken.

Motivation - cont.

- Most highly confidential information originally comes into being either as speech or as keystrokes on a PC.
- If it can be captured by the opponent at this stage, then no subsequent protective measures would help.
- This kind of an attack could be very cheap (bug).

Passive Attacks

Attacks in which the opponent makes use of whatever electromagnetic signals are presented to him without any effort on his part to create them.

Timing Analysis



This method of attack measures the time certain actions take, and infers the instructions that were executed.

This is possible due to the fact that different instructions differ in their execution time.

Timing Analysis cont.

In 1996, Paul Kocher showed that many implementations of public-key algorithms such as RSA and DSA leaked key information through the amount of time they took.

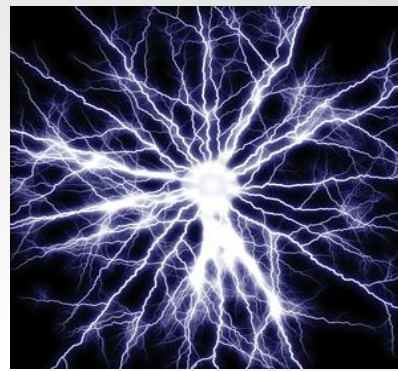
When doing exponentiation, software typically steps through the secret exponent one bit at a time, and if the next bit is a one it does a multiply.

Timing Analysis cont.

Such attacks can be prevented by using blinding.

John Kelsey, Bruce Schneier, David Wagner and Chris Hall showed in 1998 that block ciphers vulnerable to timing attacks based on cache misses.

Power Analysis



This method of attack measures the current drawn by the hardware.

Different instructions have quite different power consumption.

Power consumption also depends on the data being processed.

Power Analysis cont.

An important example is power attacks on smartcards. Adding extra components to prevent this is not usually economic.

Although the threat was known before that, Paul Kocher's "differential power analysis" is the attack that brought attention to Power Analysis.

Power Analysis cont.

Differential power analysis collects data by observing many operations of the target hardware.

DPA then uses statistical analysis to delete the noise, and extract the wanted information (keys etc.).

Power Analysis cont.

Power analysis can be combined with Timing Analysis.

For example, attacks based on cache misses can be carried out by measuring power as well as the time taken to encrypt, as a miss activates a lot of circuitry.

Power Analysis cont.

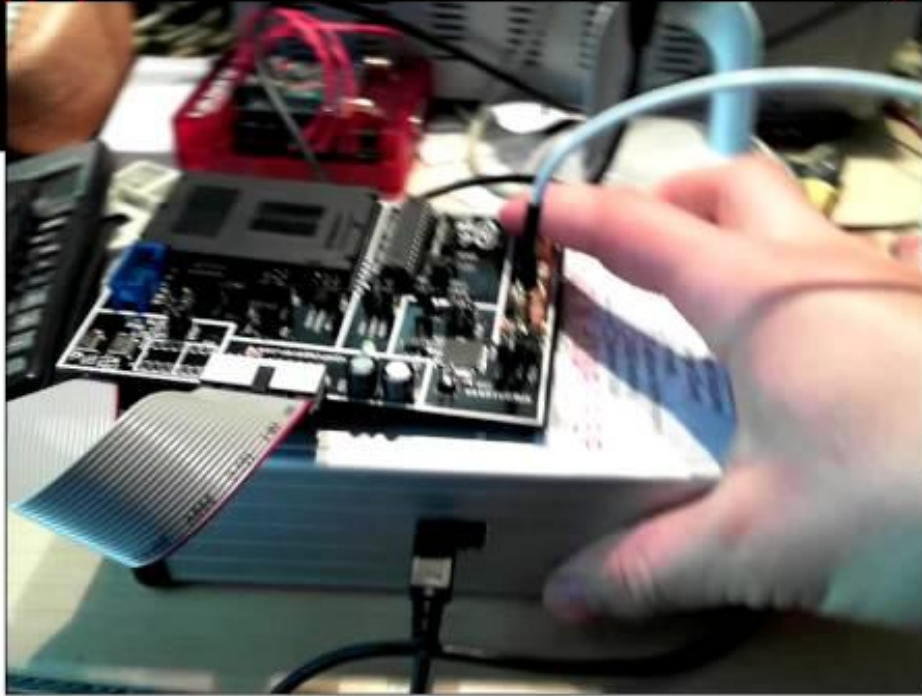
This is a noninvasive attack - the customer might not realize he was attacked.

Power Analysis - Defense

The better defense is using special hardware.

- inserting dummy operations
- using an internal clock that changes frequency once in a while.

These are not foolproof, as an attacker might use signal processing techniques to realign the power curves for averaging.



COLIN O'FLYNN

Tempest VS Hijack

Attacks can be divided into these two categories:

- Hijack - the signal is conducted over some kind of circuit.
- Tempest - the signal is radiated as radio frequency energy.

Leakage Through RF Signals

Monitors emit a weak TV signal.

This radio signal contains a distorted version of the image (unless they are specifically shielded).

Leakage Through RF Signals - cont.

Given a suitable broadband receiver, these emissions can be picked up and reconstituted as video.

The possibility of remote snooping on everything from fax machines through shielded RS-232 cables to ethernet has been established.

Leakage Through RF Signals - cont.

“Jammers” are hard (and expensive) to make and are usually not available in the commercial sector.

Leakage Through RF Signals - The Zone system

The zone system is a way to measure the level of protection against Tempest attacks.

Basically, equipment certified as Zone 0 should not emit any signals that are exploitable at a distance of one meter.

Zone 1 - 20 m, Zone 2 - 120 m, Zone 3 - 1200 m.

The Zone system - cont.

Commercial off-the-shelf equipment tends to be zone 2-3 when tested.

The zone system allows organizations to save costs by keeping most sensitive data on equipment furthest from the facility perimeter, and shield stuff only when they really have to.

The Zone system - cont.

The Zone system has cut costs but still, shielding is expensive - NATO government agencies pay over a billion dollars a year overall.

'Soft Tempest'

'Soft Tempest' is a cheaper protection against RF leakage.

It was developed by Ross Andresson and Markus Kuhn.

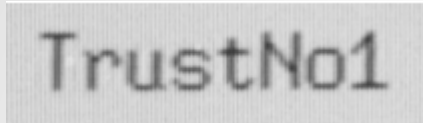
Soft Tempest uses software techniques to filter or mask the information bearing electromagnetic emanations from a computer system.

‘Soft Tempest’ - cont.

Most of the information bearing RF energy from a Monitor is concentrated in the top of the spectrum.

Soft Tempest filters out this component. It removes the top 30% of the Fourier transform of a standard font using a low-pass filter.

'Soft Tempest' - cont.



TrustNo1

Screen, normal text

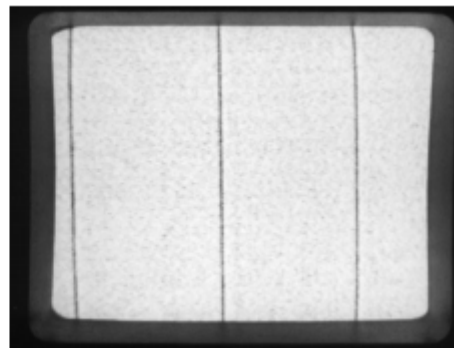


Normal text
reconstructed using a
Tempest attack



TrustNo1

Screen, filtered text



Filtered text
reconstructed using a
Tempest attack

Pictures are from
"Security Engineering"
by Ross Andresson,
chapter 17

Active Attacks

Attacks in which the opponent enhances or creates the electromagnetic signals that are emitted from the target hardware.

Tempest Viruses

It is possible to write a Tempest virus that will infect a target computer and transmit the secret data it steals to a radio receiver hidden nearby. This way an opponent could attack a computer protected by a firewall, or even not connected to a network.

Tempest Viruses - cont.

This affects the way we need to test our devices in regards to Emsec.

It is not enough to listen passively, we need to check the worst-case.

We need to see what happens when we execute the “loudest” operations.

Tempest Viruses - cont.

Edward Snowden's disclosure of NSA's classified documents reveals extensive use of tempest viruses.

One of these is codename SURLYSPAWN.

This virus logs keyboard strokes and can then send it out through RF.

This virus is part of the ANT catalog.

Nonstop

Another class of active methods.

Exploites RF emanations that are accidentally induced by radio transmitters and other RF sources (e.g. mobile phones), that are near the target device.

Nonstop - cont.

Let's say a mobile phone is used near a computer that is processing classified information.

The phone's transmitter may induce currents in the computer that get modulated with sensitive data. This can be used to eavesdrop or even harm the target equipment.

Nonstop - cont.

Ships and aircrafts are especially vulnerable to this kind of an attack as they carry many radios and radars.

Glitching

Here, the opponent inserts transients into the power or clock supply to the hardware in the hope of inducing a useful error.

E.g. replacing a single clock pulse with two much narrower pulses. This reliably causes the processor to execute a NOP, and can be used to perform a selective code execution attack.

Active Attacks - Defenses

Defending against active attacks is similar but trickier.

We can use error correction codes.

One example is using dual-rail self-timed logic, i.e. every bit is represented by 2 physical bits.

We signal '1' by '10' and '0' by '01', so '11' will trigger an alarm.

Optical, Acoustic and Thermal Side Channels

Other attacks include the use of these emanations.

e.g. recording the typing of a text on a keyboard and then using the audio to decode the text that was typed (as was done by Li Zhuang, Feng Zhou, and Doug Tygar in 2005).

Optical, Acoustic and Thermal Side Channels cont.

Tromer, Shamir and Genkin recently published a new acoustic key extraction attack. The attack can extract full 4096-bit RSA decryption keys from laptop computers, within an hour.

The Future of Emsec

The biggest threat is bugs, whose range is growing while costs are descending.

It is likely that Emsec will become a growing security issue in the private sector, as these attacks become easier (and cheaper) while defending is not straightforward.

The End