ELEC5616 COMPUTER & NETWORK SECURITY

Lecture 21:
Hardware Security

HARDWARE SECURITY

Tamper resistance in cryptography has been around for centuries:

- Naval code books were weighted so they would sink if thrown overboard.
- British Government dispatch boxes today are lead lined.
- Codes and keys for wartime cyphers were printed in water soluble ink.
- Russian one time pads were printed on cellulose nitrate which burns rapidly.
- One US wartime cypher machine came with thermite self destruct charges.

Tamper resistance devices are those that resist keys been extracted.

Tamper evident devices are those that make key extraction obvious when checked.

COMMON SECURITY FEATURES

Robust metal enclosures which act as a Faraday Cage.

Encryption hardware.

Key memory (static RAM that zeros when the case is opened).

Sensors which aid this:

- Lid or casing switches
- Light sensitive diodes, tilt switches, temperature and radiation alarms

Physical separation of serviceable components (e.g. batteries) from core of the device.

Alarms.

Potting mix (solid, opaque epoxy resin) to make reverse engineering of electronics difficult.

Tamper sensitive barriers

- Fine wire mesh or coils embedded in epoxy, wired to switches

OVERVIEW OF ATTACKS ON CRYPTO PROCESSORS

Often designs make assumptions that hardware is tamper resistant and hence secure.

This assumption is usually poor.

This is just a few things of which might go wrong:

- Key material can be stolen, leaked, obtained by bribery
- Casing can be cut through and sensors disabled
- Potting can be scraped away and probes inserted to read off data.
- If memory has been set for a long time it might be burned into the SRAM.
- RAM contents can be burned in by bathing the device in ionizing radiation.
- An attacker might freeze memory (e.g. below -20C) where static RAM will retain state after power is removed.
- Side channels (e.g. radio & optical emissions, power analysis).
- Heads of disk drives change alignment slightly, allowing data recovery.

DALLAS 5002 MICROCONTROLLER

- Security microcontroller used in EFTPOS terminals, where customer PINs are stored.
- The main security feature is bus encryption, which encrypts the address and data bus on the fly- allowing the device to operate with with external (unprotected) memory.
- Each device has a unique master key which encrypts this bus traffic, generated at random on power up.
- The software is then loaded through the serial port, encrypted.
- The device is then ready to use.
- Power for the device must be maintained to avoid a tamper event.

ATTACK ON THE DALLAS 5002

Early versions of this device fell to a cyphertext instruction search attack.

The principle is that some of the processor's instructions have a visible effect on the I/O of the chip.

In particular, there is one instruction will cause the next byte in memory to be output on one of the ports.

ATTACK ON THE DALLAS 5002

The trick is to intercept the bus between the processor and memory with a test clip and try all possible 8-bit (256) instructions, watching the ports.

Eventually the right instruction will be found.

By modification of this instruction, a simple program can be written (encrypted):

```
loop:   outb portA, (registerX++)
        jmp loop
```

The device will then faithfully dump all of memory out on the port in the clear.

SMARTCARDS

A smartcard is a self contained microcontroller, with a processor, memory and a serial interface integrated onto a single chip, packaged in a plastic card.

Smartcards are used in a variety of applications:

- Pay-TV
- Telephone cards
- Mobile phone SIMs
- Hotel door locks
- Debit and Credit cards

There are three main types of smartcards:

- Simple memory, with no processor
- Processor and memory
- Crypto processor and memory
- Cards that run a Java virtual machine

SMARTCARDS

A smartcard is primarily usually used to provide authentication functions cheaply (replacing magnetic cards)

Typical smartcard configuration:

- 8-bit processor (some now use a 32-bit ARM core or Java VM)
- Serial I/O (power, reset, clock and serial pins)
- ROM to hold program data (~16kB)
- EEPROM to hold customer specific data (~16kB)
- RAM to hold transient computation data (~256B)
- An operating system that may allow additional programs to be loaded on to the card. The two most widely used operating systems are MULTOS and JavaCard.

Many smartcards today are also contactless

- Though many of these are simple memory / ID cards.

ATTACKS ON SMARTCARDS

Protocol attacks

Early Pay-TV cards let subscribers access all channels for an introductory period, then signals were sent over the air to cancel channels not paid for.

A man-in-the-middle attack on this was to simply ignore these messages.

Attacks on the power supply

Early smartcards received Vpp (the programming voltage for EEPROM) on an external pin. An attacker only need remove this contact (e.g. cover with sticky tape) and EEPROM can never be written to (such as trying to reduce credit on a telephone card).

Power analysis attacks which is observation of instructions being performed by a processor by looking at the amount of current it draws (each unique instruction drives a unique configuration of transistors).

Inferential & Differential Power Analysis

Physical attacks on the packaging

Removing the thin glass layer on the chip, the potting mix and so on, and probing the device.

ATTACKS ON SMARTCARDS

Attacks on the clock

Slowing the clock down so instructions are executed one step at a time and the smartcard surface or power usage can be analysed to determine what instructions are executed.

A memory linearisation attack

Damaging the instruction bus so that particular instructions are executed (in sequence to arbitrarily dump memory, for example).

Reverse engineering attacks

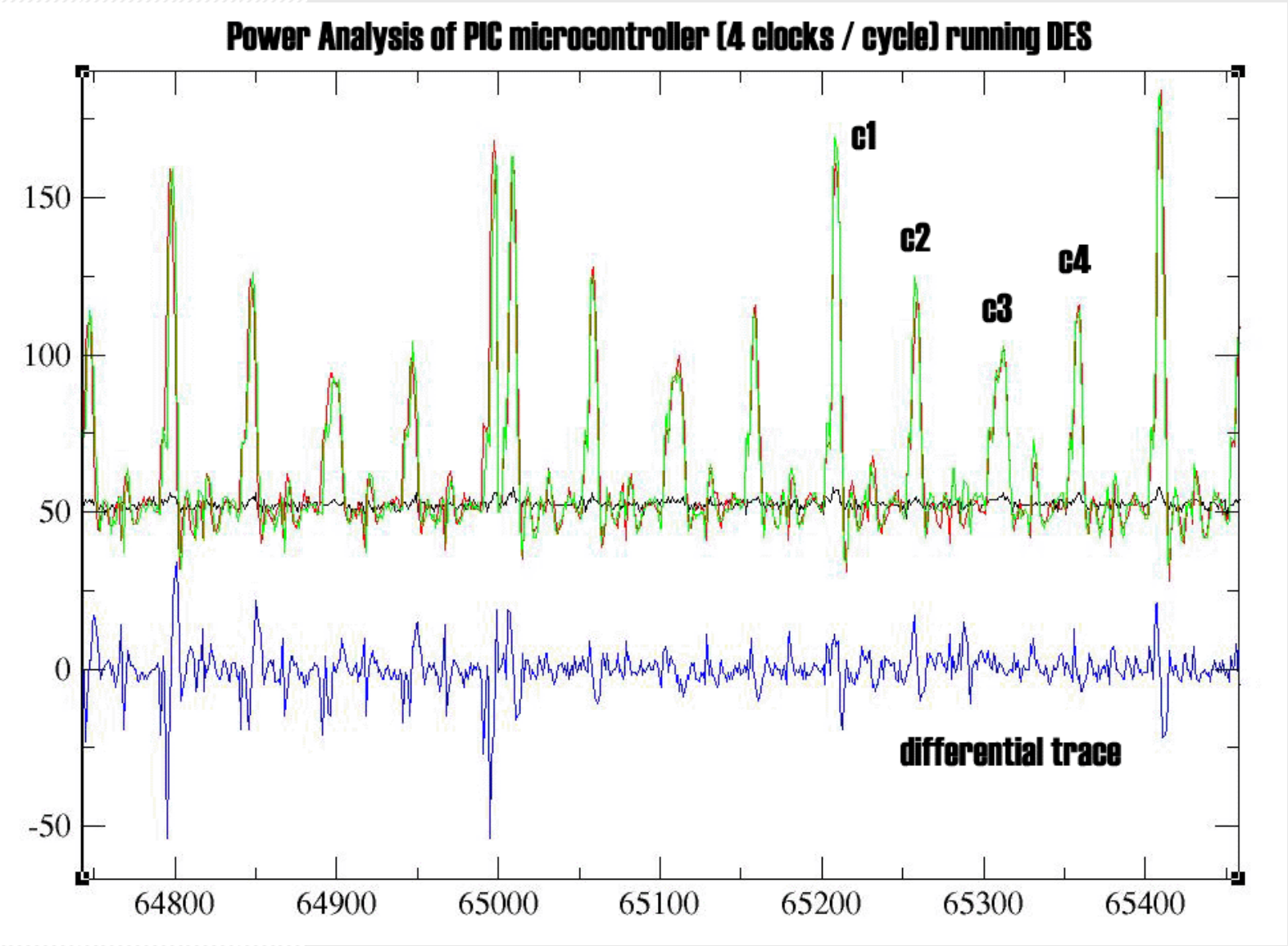
Manually reconstructing crypto processor circuit layouts from micrographs.

Pay a commercial chip reverse engineering company to do it for you (often done to check patent infringements).

Chipworks is an example (http://www.chipworks.com).

Attacking the surface mesh

Using a Focused Ion Beam Workstation (FIB), holes can be drilled, and insulators and conductors laid down as desired allowing the mesh to by bypassed.



Source: Ryan Junee [USYD]

EMISSION SECURITY

Emission security refers to preventing a system from being attacked by using compromising emanations (conducted or radiated electromagnetic signals).

Often cited is TEMPEST, which is a military term for defenses against stray RF from computers and video monitors.

Other attacks involve viewing the optical spectrum [Kuhn].

EXAMPLES OF EMISSIONS

Crosstalk in cabling.

In Britain, stray RF leaking from oscillators in TV sets is used to track people down who don't have a "TV license".

Information leakage through sidebands

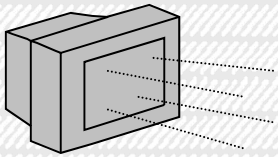
e.g. In 1960, MI5 noticed in surveillance of the French embassy that the plaintext from a cypher machine was being leaked on a sideband.

Van Eck monitoring of VDU signals.

Glitching / differential fault analysis

Clock lines, power lines, parity bits.

OPTICAL EMISSIONS



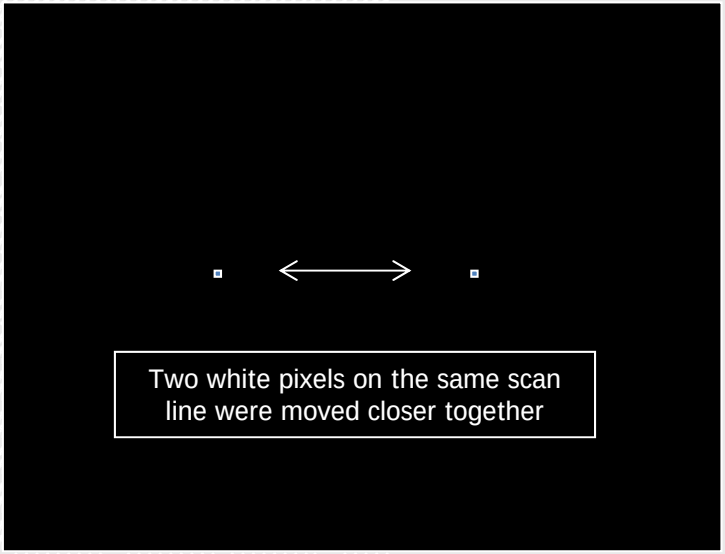
Diffuse reflections of information carrying emissions can be detected

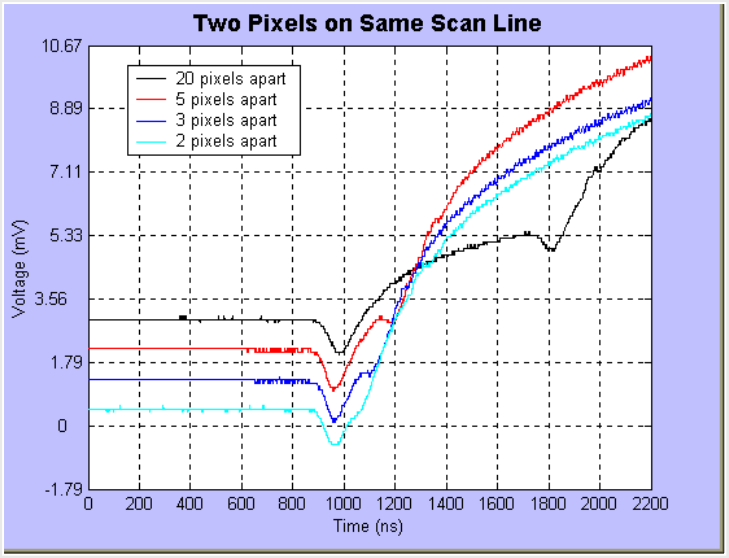
CRT raster scan display monitor

Photomultiplier tube

High speed CRO

Computer for signal capturing and processing





Source: Liz Eykman [USYD]

CONCLUSION

No technology or combination of technologies can make hardware resistant to penetration by a determined and skilled attacker (again “raising the bar”).

There are lots of graduate students in EE & CS in the world with lots of spare time on their hands.

Often failures are not with the hardware itself, but some other facet of the system (e.g. users, interfaces with other devices).

Do not trust manufacturer’s claims about security. Hardware vendors have a particularly poor track with security.

Tamper resistance should be an added layer of security, not a single point of failure for the system.

CONCLUSION

Avoid global secrets.

Use fault-tolerant machine code.

Clever protocols / system design can reduce the importance of tamper resistance.

Implement fallback modes, intruder detection and identification, counter measures.

Like all systems, subject it to open third-party review.

REFERENCES

Security Engineering

§14 - §15

Papers (For interest):

A Practical Introduction to the Dallas Semiconductor iButton [Kingpin]

Tamper Resistance, a Cautionary Note [Anderson / Kuhn]

Optical Time-Domain Eavesdropping Risks of CRT Displays [Kuhn]

Differential Power Analysis [Kocher et. al]

Cipher Instruction Search Attack on the BusEncryption

Security Microcontroller DS5002
(http://www3.informatik.uni-erlangen.de/Publications/Articles/kuhn_ToC.pdf)