Smartcards
and RFID

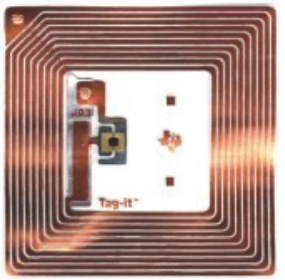
IPA Security Course

Lejla Batina & Erik Poll
Digital Security
University of Nijmegen

Overview

- example uses
- (security) functionality
- smartcard technicalities
- RFID technicalities
- attacks

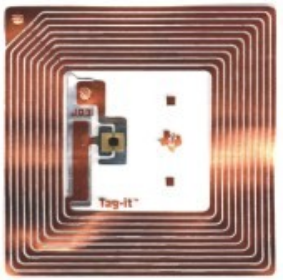
Smartcard & RFID uses



Example smartcard & RFID uses

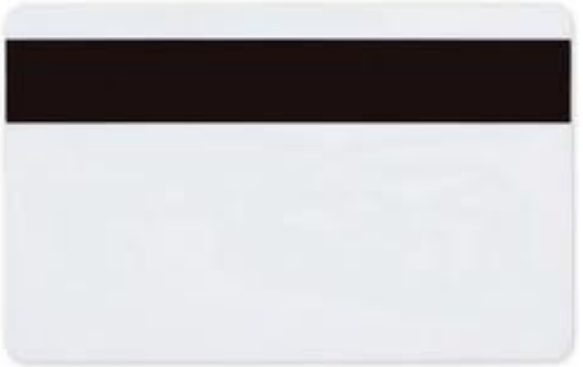
- bank cards
- SIMs in mobile phone
- public transport
  - eg OV chipkaart in NL
- identity documents
  - modern passports and national ID cards contain (contactless) chip
- access cards
  - to control access to buildings, computer networks, laptops,…
  - eg Rijkspas for government personnel
  - eg UZI pas for medical personnel to access EPD
- pay TV

(Security) functionality



Differences? Commonalities?

With respect to functionality or security



Differences & Commonalities

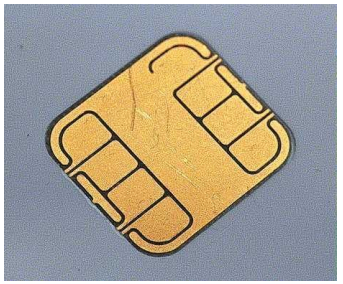
- all provide data storage
  - for reading and/or writing
- but secured to different degrees & in different ways
  - different aims of securing:
    - confidentiality
    - integrity/authenticity
  - different ways of securing
    - integrity by physical characteristics vs digital signatures
    - access control (eg PIN code, password, crypto protocol) possible on smartcard, not on a magstripe

Differences? Commonalities?

Smartcard vs other computers

- No fundamental difference !
  - smartcard does not only offer data storage but also processing power
  - Btw, smartcards outnumber normal computers such as PCs and laptops
- Smartcard is *restricted* in its possibilities
  - *How, for example?*
- Smartcard can offer *security* that PC cannot
  - *What, for example?*
    - *eg you cannot remove the hard drive*

Smartcard technicalities



What is a smartcard?

- Tamper-resistant computer, on a single chip, embedded in piece of plastic, with very limited resources
  - aka *chip card* or *integrated circuit card (ICC)*

- capable of "securely"
  - storing data
  - processing data
    - This processing capability is what makes a smartcard *smart;* stupid cards can store but not process
    - NB processing capabilities vary a lot....

What does "securely" mean?

- Functionality (software) and data on the card cannot be "messed with"
- The smartcard can implement access control to restrict access to data or functionality, eg
  - deny possibility to read or write some data
  - only allowing it after entering password or PIN code
  - only allowing it after performing some security protocol
- The smartcard can implement cryptographic checks to ensure confidentiality or integrity, eg
  - encrypt / sign data it provides
  - decrypt / check signatures on data it receives

Form factors for smartcards

- traditional credit-card sized plastic card
  - ISO 7816

- mobile phone SIM
  - cut-down in size

- contactless cards
  - aka *proximity card* or *RFID transponder/tag*
  - also possible: dual interface

- iButton

- USB token

3 types of functionality

1. *stupid card* just reports some data

   eg card shouts out a (unique) serial number on start-up

2. *stupid smartcard* aka memory card

   provides configurable file system with access control

   by means of *PIN code/passwords* or *crypto keys*

   or even simpler: *irreversible writes*

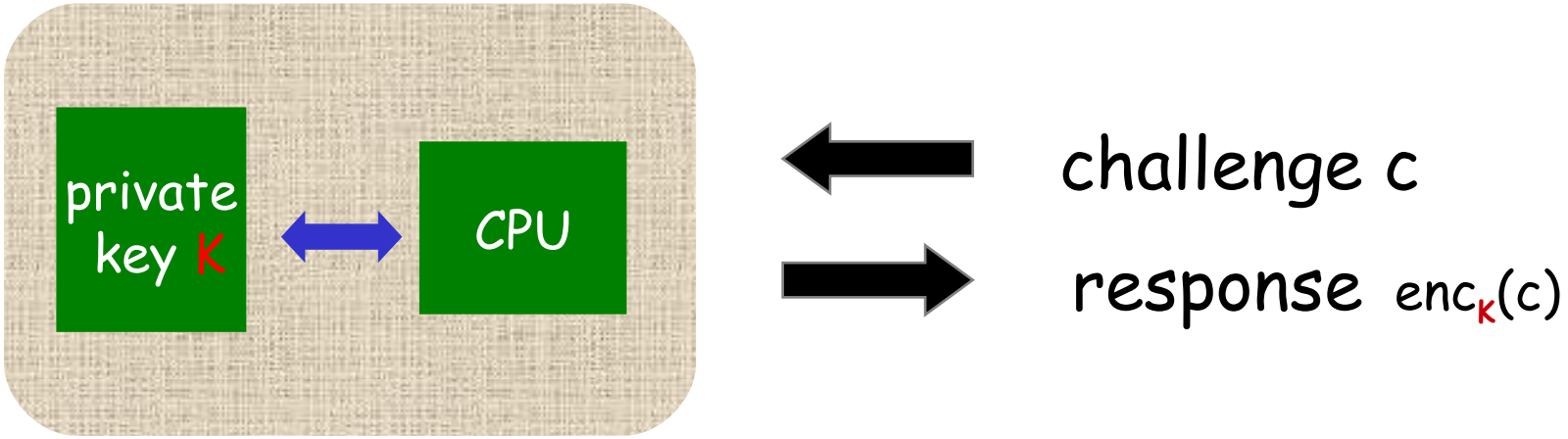
3. *smart smartcard* aka microprocessor card

   provides programmable CPU that can implement any functionality

   eg complicated security protocols

What type of attacks can 2 & 3 withstand that 1 can't?

Typical use of smartcard for authentication



- If card can perform encryption, then private key K *never* leaves the card
- This scheme can also be used for non-repudiation, ie signing.
- The issuer does not have to trust the network, the terminal, or card holder

Smartcard hardware

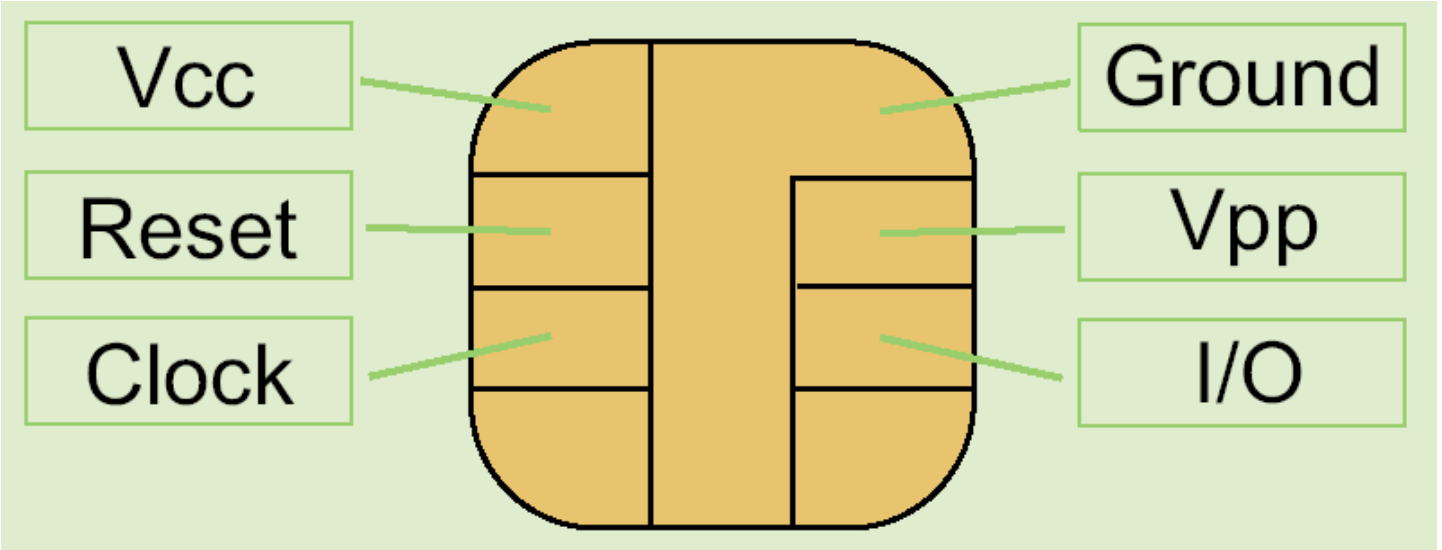
- CPU (usually 8 or 16, but now also 32 bit)
- possibly also
  - crypto co-processor & random number generator (RNG)
- memory: volatile RAM and persistent ROM & EEPROM
  - EEPROM serves as the smartcard's hard disk
- no power, no clock!

A modern card may have 512 bytes RAM, 16K ROM, 64K EEPROM and operate at 13.5 MHz

Important reason for low capabilities: cost!

Also, keeping smartcard simple means we can have high confidence; you don't want Windows 7 as operating system on a smartcard

Contact cards (ISO 7816-2)



External power supply and external clock

- Originally 5 V, now also 3V or 1.8V
- Vpp - higher voltage for writing EEPROM - no longer used as it introduces a serious security weakness

Multi-application & post-issuance

Old-fashioned smartcards contain one program, that can never be changed

Modern smartcard platforms

- are multi-application, ie allow multiple, independent programs (aka applets) to be installed on one card
- allow post-issuance download: applications to be added (or removed) after the card has been issued to the card holder

Of course, this is tightly controlled - by *digital signatures*

Examples of such platforms: JavaCard and MULTOS

Application management using the GlobalPlatform standard

Multi-application cards

- Multi-application vision: everyone carrying *one* card, with all their smartcard applications
- This is not going to happen. Problems:
  - trust

    banks won't allow untrusted programs of others on their cards; or allow their programs to be seen by others
  - marketing

    who gets to put their logo on the plastic?
- Still, multi-application is useful for development & card managament by a single vendor
  - eg used to add services to SIMs that are out in the field

The terminal problem!

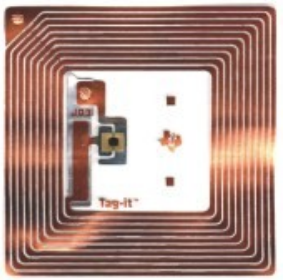
- THE fundamental problem with smartcards
  no trusted I/O between user and card
  - no display
  - no keyboard

- *Why is this a problem?*
- *Is this a problem for card holder or card issuer?*

Solutions:

- Card with built-in display & keyboard
- Alternative: give people a reader

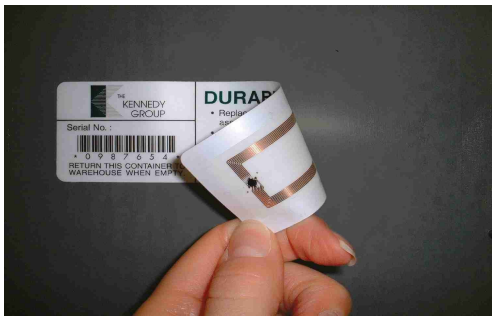
RFID technicalities



RFID

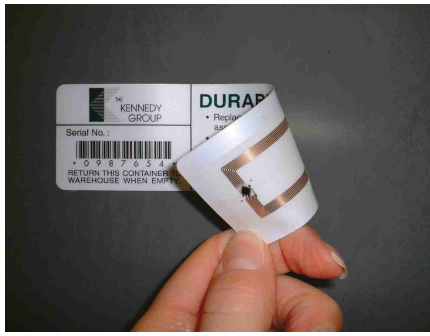
- RFID = Radio-Frequency IDentification
- RFID devices are called tags or transponders
- "smartcard chip with an antenna"
- Often not so smart: RFID tags are often stupid cards (type 1&2)
  - simplest tags only support data transfer from tag to reader

Powerful RFID tags are also called contactless smartcards



Many types of RFID tags

- with different read ranges & capabilities, operating at different frequencies
- Many just transmit a fixed code when activated:
  - Animal identification RFID tags
  - Item management - RFID bar codes (Global TAG)
  - Container identification - with battery for large range
  - Anti-theft systems - one bit of information
- More advanced cards include proximity cards (ISO14443)
  - read range less than 10 cm
  - eg MIFARE and contactless smartcards (such as e-passport)



NFC = Near Field Communication

- Implemented in mobile phones
  - compatible with ISO14443 proximity cards
- Phone can act as reader (active mode) or as a tag (passive mode)
- The next big thing in the mobile phones?

A consortium of the large Dutch banks and telco's (Sixpack/TRAVIK) is developing an NFC payment solution (where payment applet is added on mobile phone SIM). First example of real multi-application cards?

Pros & cons of contactless over contact?

- advantages
  - ease of use
  - no wear & tear of contacts on card and terminal
    - less maintenance
    - less susceptible to vandalism
- disadvantages
  - easier to eavesdrop on communication
  - communication possible without owner's consent
    - for replay, relay, or man-in-the-middle attacks (more on that later)
  - RFID tags often have more limited capabilities to provide security
    - eg amount of data, crypto

passive vs active attacks on proximity cards

passive attacks

- eavesdropping on communication between card & reader
- possible from several meters

active attacks

- unauthorised access to card without owner's knowledge
- possible up to ≈ 25 cm
  - activating RFID tag requires powerful field!

- aka virtual pickpocketing
- variant: relay attack

(Scaremongering?) story about passport bombs
http://www.youtube.com/watch?v=-XXaqraF7pI

Privacy

- RFID introduces obvious privacy risks
  - RFID barcode may provide unique ID for an individual product

Anti-collision

- anti-collision protocol needed for terminal to select one card to talk to, if several cards are in the field of a reader
- for this, cards send out a number for the reader to identify them

This anti-collision leaks information & may cause privacy concerns

- eg test version of Dutch passport used a *fixed* number in the anti-collision protocol. Real one uses random number
- Italian e-passport still have a fixed & unique number here

Remaining e-passport problems…

- Error messages of the e-passport reveal manufacturer
  - ie provide fingerprint

deVerdieping
Trouw

• Legio criminele toepassingen

Na ov-chip nu ook lek in paspoort

De chip in het nieuwe Nederlandse paspoort en andere passen is 'lek'. Dieven kunnen snel zien of iemand een paspoort bij zich heeft en uit welk land hij komt.

Vincent Dekker

Moderne paspoorten in tassen of binnenzakken verraden draadloos hun aanwezigheid én uit welk land ze komen. Onderzoekers van de Radboud Universiteit in Nijmegen hebben een beveiligingslek ontdekt in de chip die de pas juist veiliger moet maken.

„We hebben op de universiteit studenten van tien nationaliteiten en bij allen kunnen we ongezien zeggen uit welk land hun pas komt", aldus Erik Poll, die samen met Wojciech Mostowski en Henning Richter het beveiligingsprobleem ontdekte. In ieder geval paspoorten uit Nederland, Australië, België, Duitsland en

antwoorden op elke correcte vraag van een officieel leesapparaat, zoals bij de douane. Maar men is vergeten dat ook te regelen voor antwoorden op verkeerde vragen. In de praktijk blijkt dat elk land een eigen manier heeft bedacht om met foute codes om te gaan. Analyseer de foutmelding die je terugkrijgt na het bewust versturen van een verkeerde code en je weet uit welk land het paspoort komt."

Foutmeldingen verraden veel over de werking van computers en zijn al vaak gebruikt om systemen te kraken. Daar heeft de Icao echter niet genoeg bij stilgestaan, blijkt nu.

De chip in het paspoort werkt, net als die in bijvoorbeeld de gekraakte OV-chipkaart en toegangspasjes, met de draadloze rfid-technologie. Daardoor is een rfid-lezer van een paar tientjes genoeg om de paspoorten te herkennen. Om ze geschikt te maken om op afstanden van 25 centimeter te werken, in plaats van de standaard van enkele centimeters, hoeft er alleen maar een grotere an-

Olympische fakkel San Francisco volg

Na Londen ontaardde ook in Parijs de olympische fakkeltocht door Tibetprotesten in chaos. De volgende steden maken hun borst al nat.

Van onze redactie buitenland

De olympische vlam verliet gisteravond Parijs, op weg naar de volgende bestemming: San Francisco. Maar sommige officials beginnen zich vanwege alle Tibetprotesten af te vragen of de estafette wel door moet gaan.

De route van de vlam door Parijs werd gisteren ingekort. De protesten tegen het Chinese ingrijpen in Tibet veroorzaakten dermate veel chaos dat de fakkel liefst vijfmaal gedoofd moest worden – volgens de organisatoren één keer vanwege een defect en vier keer uit voorzorg. De olympische vlam bleef volgens hen wel permanent branden in een busje. Maar de chaos werd zo groot dat de route moest worden verlegd en een bezoek aan het Parijse stadhuis helemaal werd afgeblazen.

Rond tien uur vertrok het vliegtuig uit Parijs. In San Francisco stonden de volgende demonstranten al klaar om de Chinese omgang met Tibet aan de kaak te stellen. Gisteren klommen er alvast drie langs de kabels de Golden Gate Bridge omhoog, waarna ze een spandoek ontrolden met 'Bevrijd Tibet' erop. En presidentskandidate Hillary Clinton riep

Different error response of e-passports

B0 means "read binary", and is only allowed after Basic Access Control

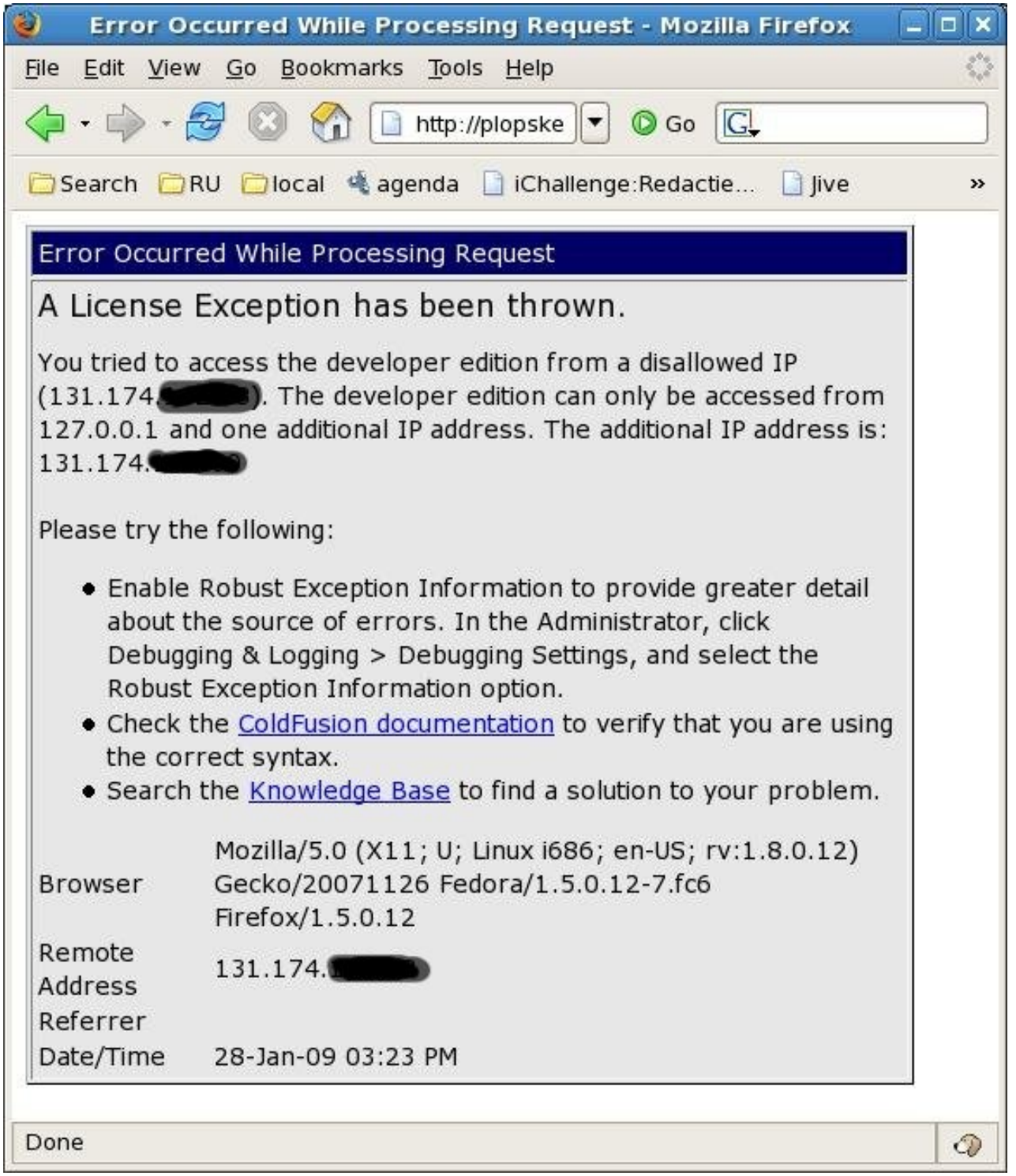
	2 byte error response	meaning
Belgian	6986	not allowed
Dutch	6982	security status not satisfied
French	6F00	no precise diagnosis
Italian	6D00	not supported
German	6700	wrong length

255 other instructions to try,
and we can try different parameters ...

This is more general problem: errors can leak information

```
An Error Has Occurred.

Error Message:

System.Data.OleDb.OleDbException: Syntax error
  (missing operator) in query expression
  'username ''' and password = 'g''.

System.Data.OleDb.OleDbCommand.ExecuteCommandTextError
  Handling (Int32 hr) at

System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSi
  ngleResult (tagDBPARAMS dbParams, Object&
  executeResult) at
```

Error report of our department online course schedules



Smartcard attacks

Classification of attacks

- cost
  - time
  - equipment
  - know-how
- tamper-evidence
  - ie can the card, card holder, or card issuer see a card is being or has been messed with?
- impact for the organisation
  - and business case for the attacker

The attacker's business case

ie. the motivation for professional attacker!

The hobbyist is after fame or publicity, the professional is after money!

Which smartcard most interesting to "hack"?

SIM, Chipknip, bank- or creditcard, pay TV

Here by "hack" we mean access private keys on the chip to clone cards

Most interesting: PayTV, Chipknip?

Least interesting: SIM card?

Classification of attacks

An attacker can target

1. organisation: eg. issuance & usage process
2. cryptographic *algorithms*
3. cryptographic *protocols*
4. software, on smartcard or terminal-side
5. the smartcard itself
   - eg. side-channel attacks or invasive attacks

} logical attacks

\

Attacking the crypto

- Difficult for standard algorithms (DES, AES, RSA, ECC, …)
- Homemade, *proprietary* cryptographic algorithms are routinely broken, eg
  - Crypto-1 used in MIFARE Classic
  - COMP128 and A5/1 used in GSM
  - Keeloq used for car keys

google for MIFARE on youtube

Common problems with crypto keys..

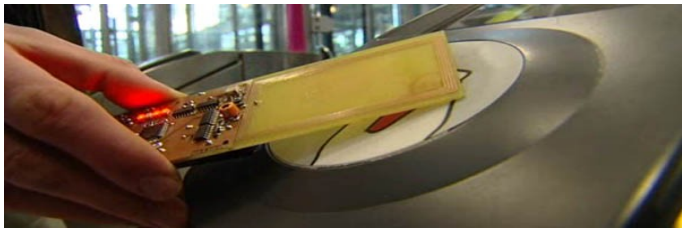
You can easily check that people use proper cryptographic algorithms, but not that people use it properly…

Common problems:

- system integrators using the same key in all cards
  - for one customer, or - worse - all their customers!

- worse still, using the default keys
  - **75%** of MIFARE applications was found to use default keys or keys used in examples in documentation
    [Source: Lukas Grunwald, DEFCON14, 2007]
  - A0A1A2A3A4A5 is an initial transport key of MIFARE tags. Googling for A0A1A2A3A4A5 produces links to documentation with other example keys to try!

Attacking the protocols



- Replay attack

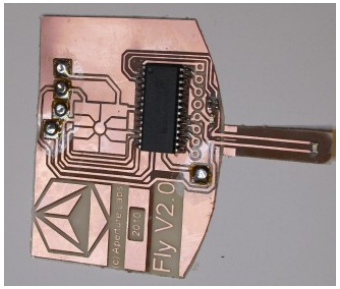
  record communication between card & terminal, and replay it

  - Eg this works for disposable ov-card

- Man-in-the-Middle attack

  intercept *and modify* the communication

  - shim can be placed inside a terminal to do this

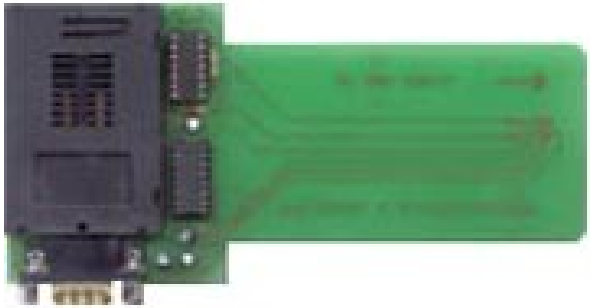


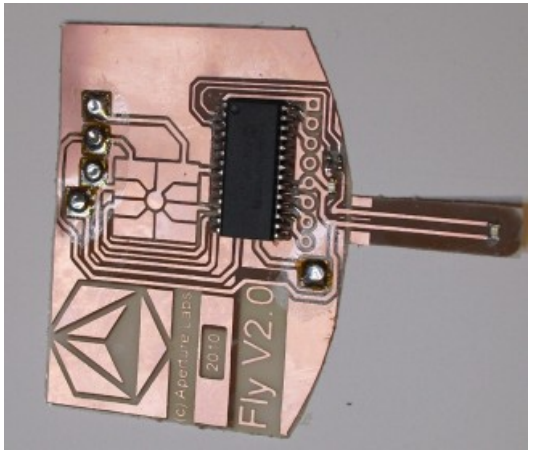
- Relay attack

  intercept communication and relay it to a different terminal

  - Eg from hacked PIN terminal in mafia-operated shop to an ATM
  - *NB much harder to avoid than replay or MITM attacks!*
  - *How does the terminal problem play a role here?*

Tools for protocol analysis



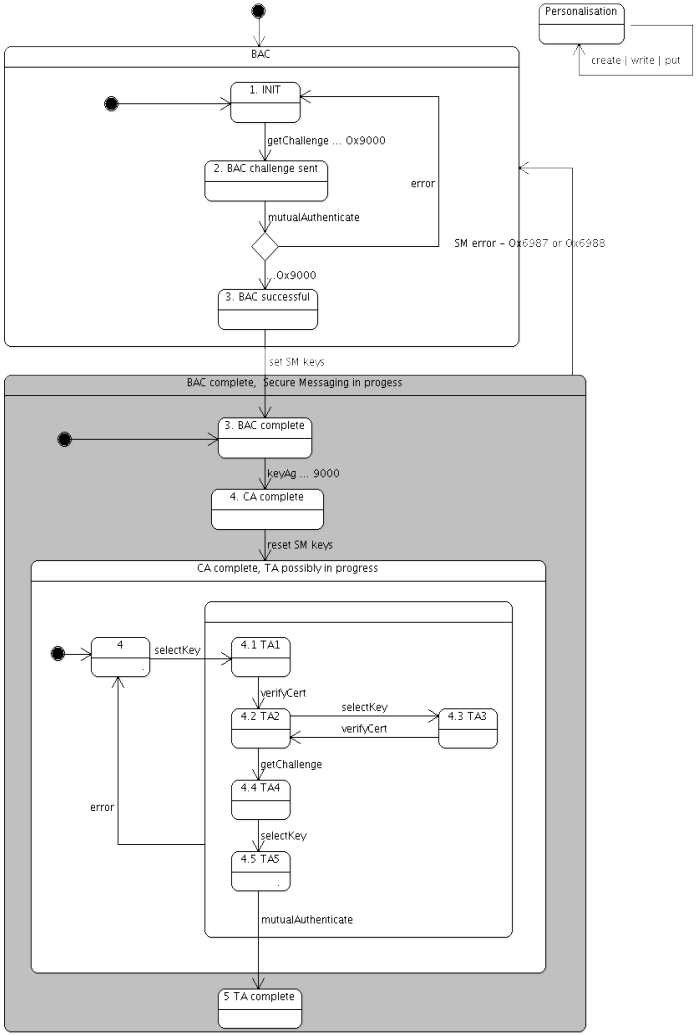


Protocol implementation errors?

- Even if the protocol is secure, an implementation could introduce bugs..
- One way to find such bugs

  model-based testing

- More ambitious: formal verification of the software to prove compliance



Example protocol attacks: EMV

EMV (EuroPay/Mastercard/Visa) is the (complicated!) international standard for smartcards used in banking.

Protocol worries so far

1. cheaper EMV cards can still be cloned
   - the chip provides signed data to authenticate, and not a challenge-response protocol (like disposable ov-chipkaart)
1. in UK: card can be used without PIN (by fooling terminal into thinking hardwritten signature is used)
2. Newer cards use encryption to communicate PIN, but a shim can force rollback to unencrypted PIN
   - We succesfully tried this ☺, but Rabobank detects this in real time ☹

Attacking the terminal (software)

- Lukas Greenwald managed to crash e-passport terminals by sending a malformed JPEG
  - causing a buffer overflow in the graphics library

- Melanie Rieback (VU) mase a SQL injection virus in a RFID tag

- *Smartcards and RFID tags should be treated as untrusted inputs*
  - *until we have authenticated the card or the data that they provide*

Attacking the terminal (software): the ov-chip

The disposable ov-chipkaart (MIFARE Ultralight) has 6 bytes of one-time programmable (OTP) memory

- initially filled with 0's; writing a 1 is an irreversible operation

Two bytes are used to invalidate tickets

- initially 00F0
- set to F8FF to invalidate tag

We can still change an invalid tag so terminals will accept it as valid; can you guess the flaw?

- flip the remaining 3 bits, so that it become FFFF

This flaw in terminals has since been fixed

side channel attacks

Smartcard attacks

So far we discussed logical attacks (100$) to exploit flaws in
- crypto, security protocol, or the software

Other possibilities
- Side channel attacks (5K$)
  - passive: power or timing analysis
  - active: fault injection (glitching or laser attacks)
- Physical attacks (100K$)
  - reverse engineering
  - probing, focussed ion beam, ...

These attacks may also be combined

Invasive vs non-invasive

- Logical & side-channel attacks are non-invasive
  - violate tamper-resistance *and* tamper-evidence
  - *can happen in a few minutes in mafia-operated shop or a tampered terminal*

- Physical attacks are always invasive
  - tamper-evident, so only violate tamper-resistance
    - ie you destroy a few chips in the process
  - *requires hours to weeks in laboratory*

Side-channel analysis

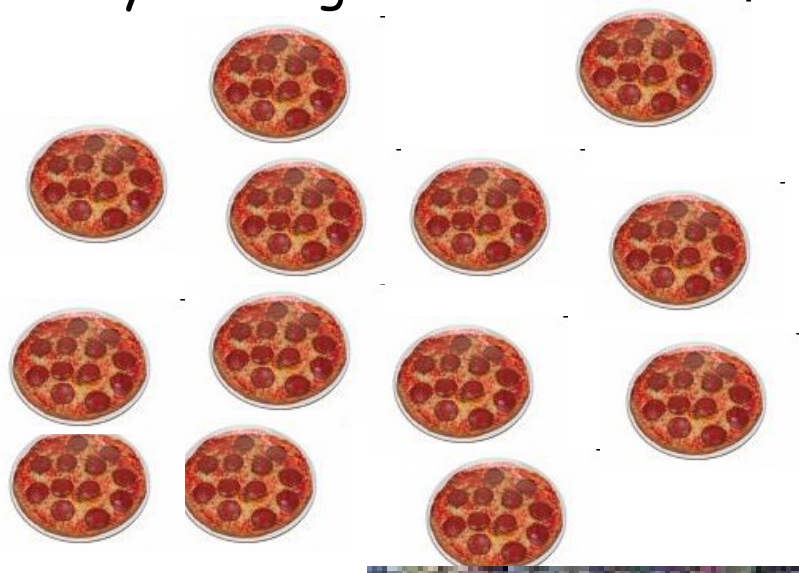
example side channel:

pizza deliveries to the Pentagon

Side-channel analysis

monday evening

tuesday evening



What evening is the invasion taking place?

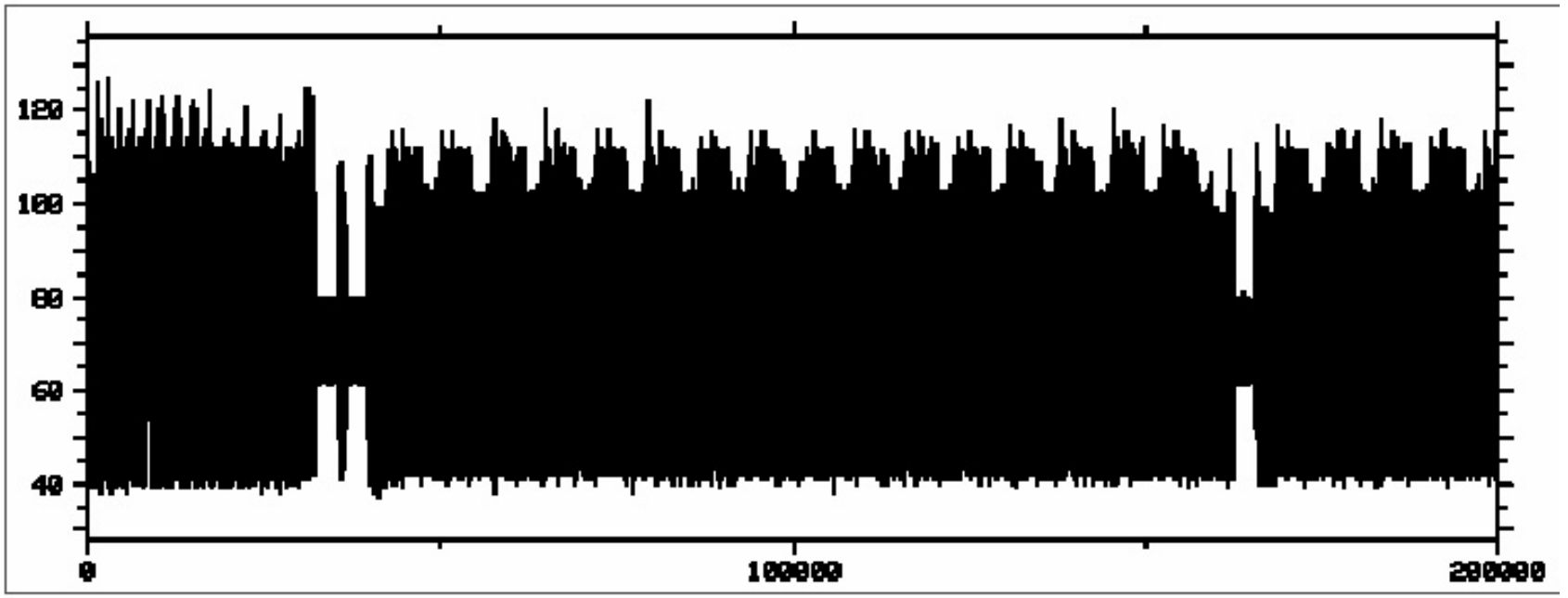
Side-channel analysis

- Side-channel = any other channel than the normal I/O channel that may be observed

- Possible side-channels:
  - power consumption
  - timing
  - electro-magnetic radiation
  - ....

Very powerful !

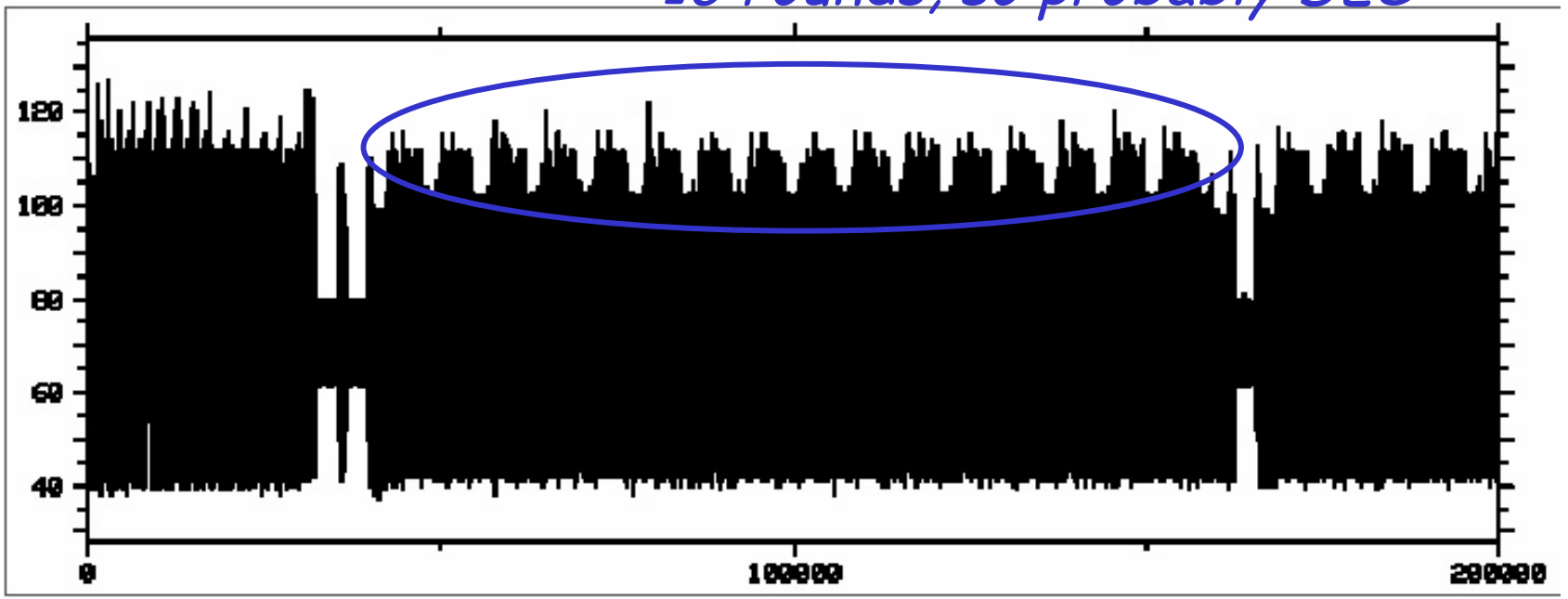
Power consumption of a smartcard



What is this card doing?

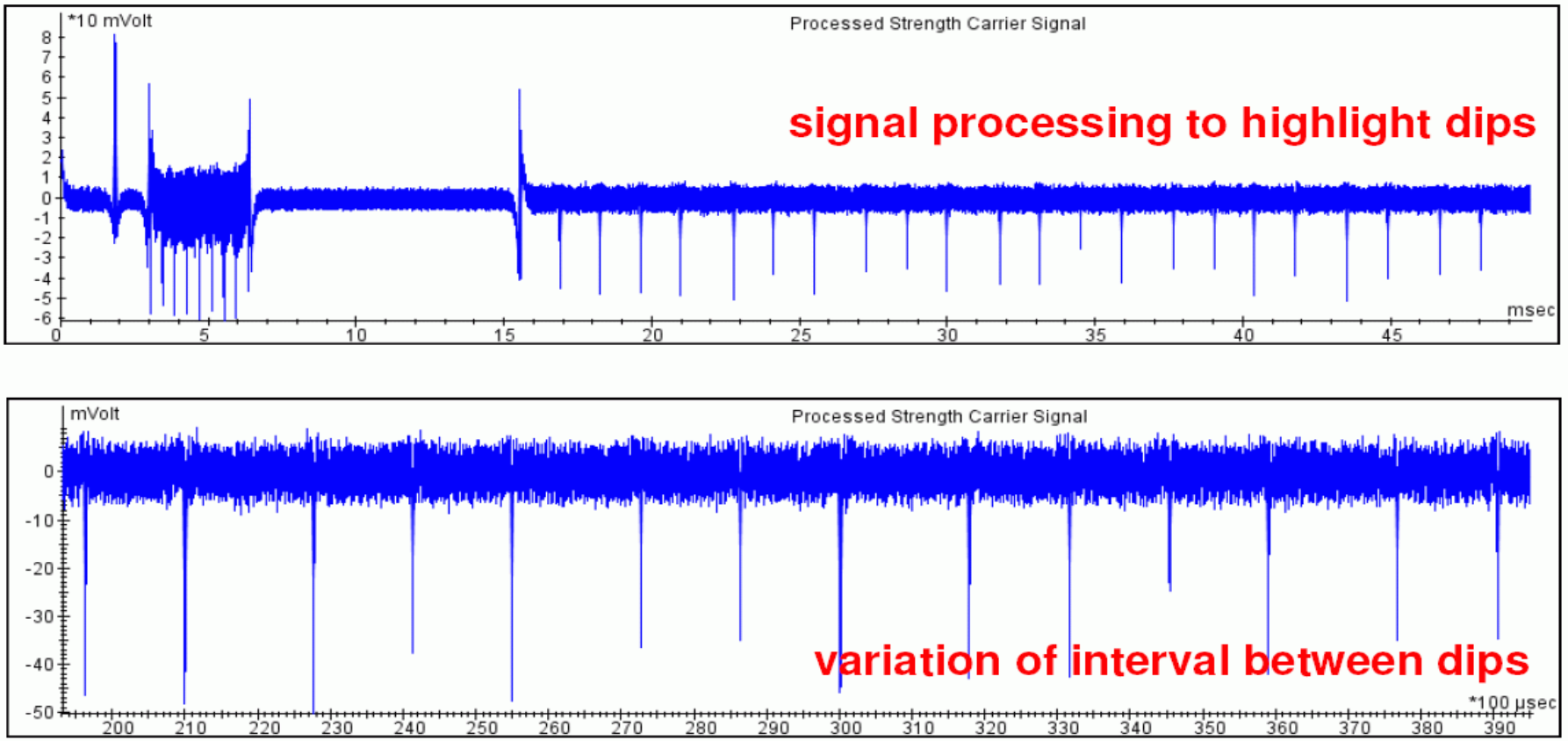
This is a DES encryption!

16 rounds, so probably DES



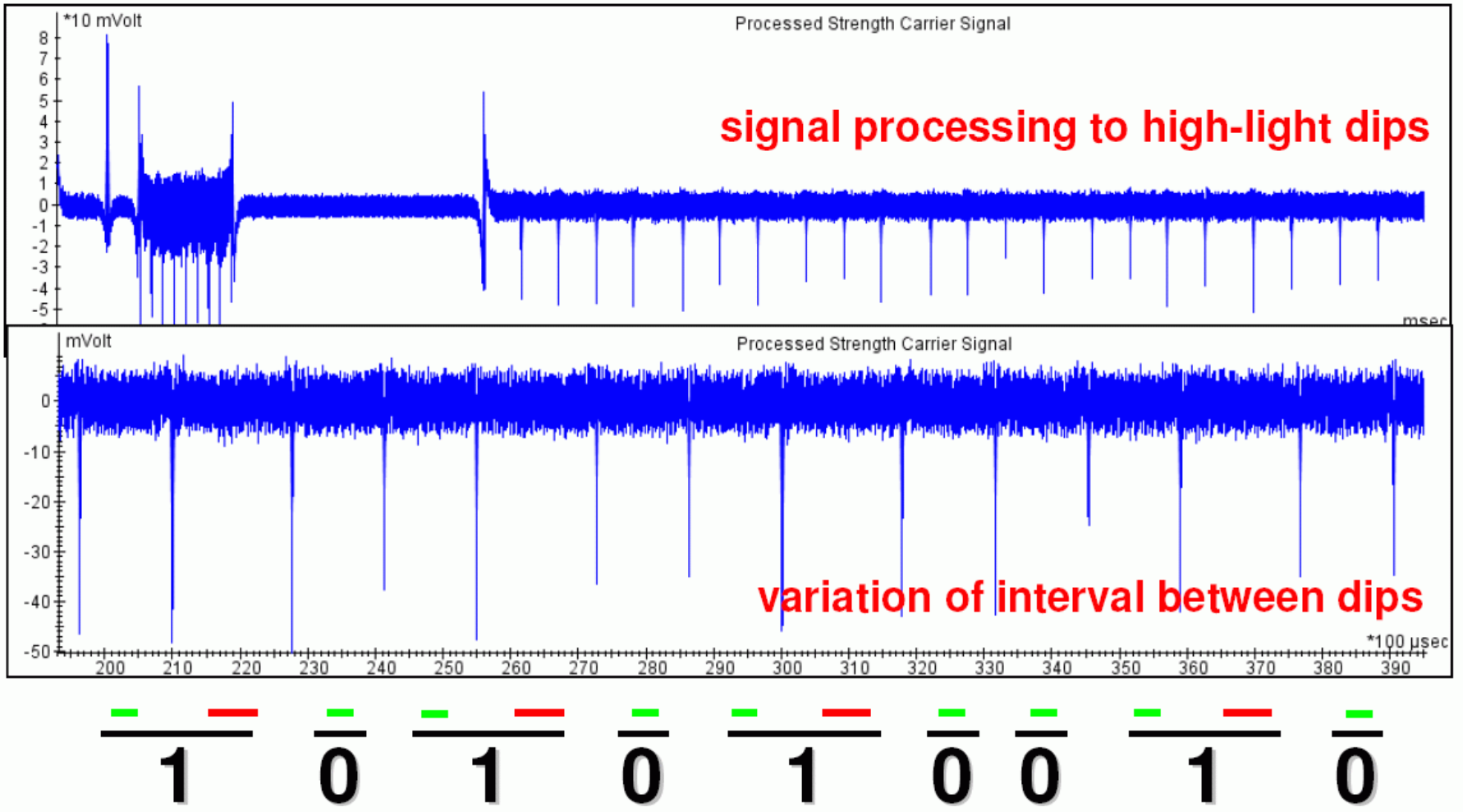
What is the key?

Power trace detail of RSA encryption



Source: presentation by Fred de Beer of Riscure at Safe-NL, June 2006

SPA: reading the key from this trace!



Source: presentation by Fred de Beer of Riscure at Safe-NL, June 2006

Power Analysis

- Simple Power Analysis - SPA
  - analyse an individual power trace
    - to find out the algorithm used
    - to find the key length
    - worst case: to find the key
- Differential Power Analysis - DPA
  - statistically analyse many power traces to find out the key

DPA has been the most serious threat to smartcards in the past 10 years!

This can also be combined with introducing faults, eg by shooting a laser

Equipment for side-channel analysis

Attacks with fault injections

Faults may be introduced as part of attacks

- card tears removing the card from the reader halfway during a transaction
  - *homework exercise: try this when charging or paying with your chipknip!*
- glitching temporarily dipping the power supply
  - eg to prevent EEPROM write after trying a PIN code
- light attacks shoot at the chip with a laser
  - to flip some bits...

Physical/invasive attacks

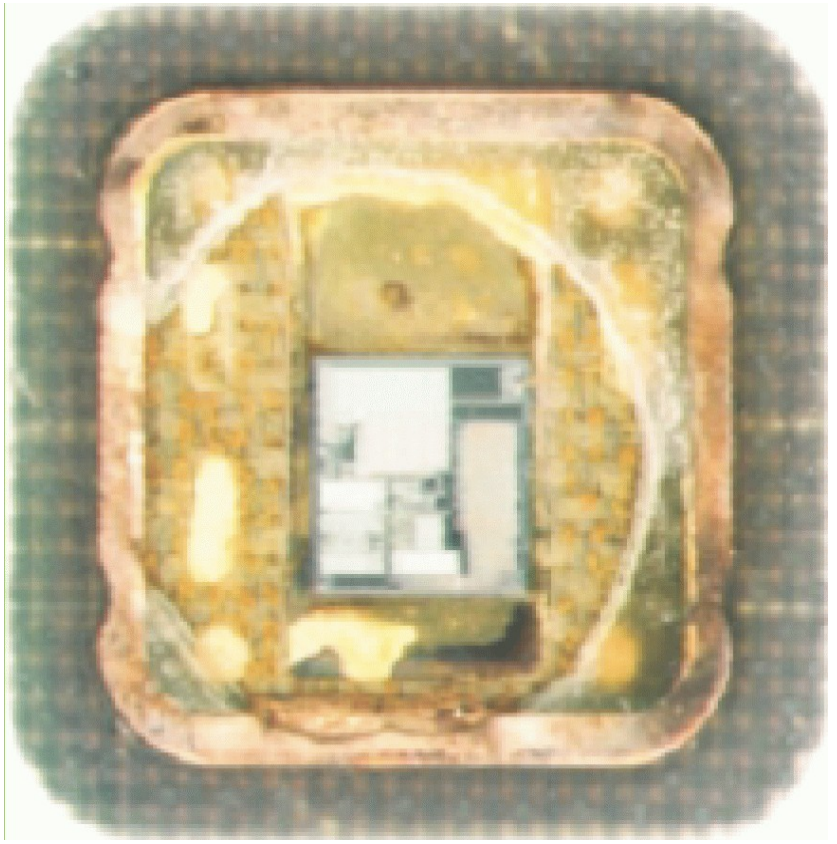
Physical, invasive attacks

- Much more costly than logical or side channel attacks.
  - expensive equipment + lots of time & expertise
- Also, you destroy a few chips in the process...

Examples

- probing
- fibbing
- reading memory contents
- ...

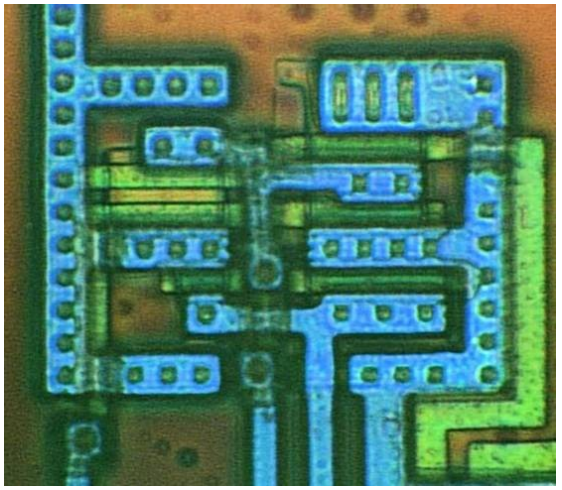
First step: removing chip from smartcard

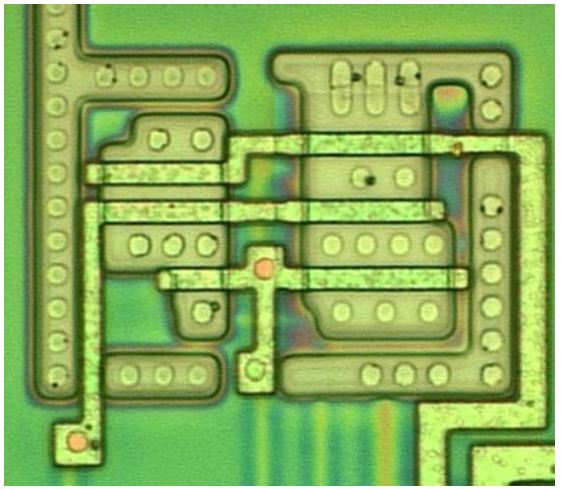


using heat & nitric acid

[Source: Oliver Kömmerling, Marcus Kuhn]

Optical reverse engineering





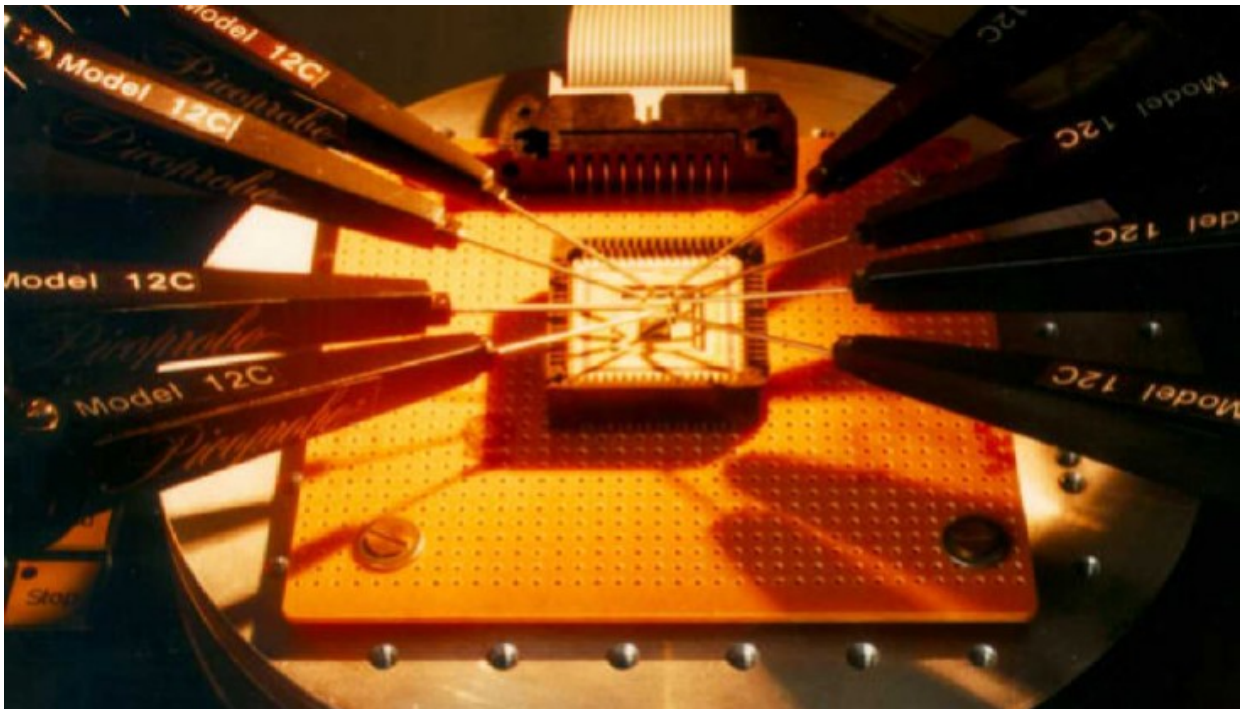
microscope images with different layers in different colours, before and after etching

[Source: Oliver Kömmerling, Marcus Kuhn]

Physical attack: probing

- Observe or change the data on the bus while the chip is in operation.

eg to observe key



probing with
8 needles

Probing can be done using physical needles (>0.35 micron) or electron beam

Probing countermeasures

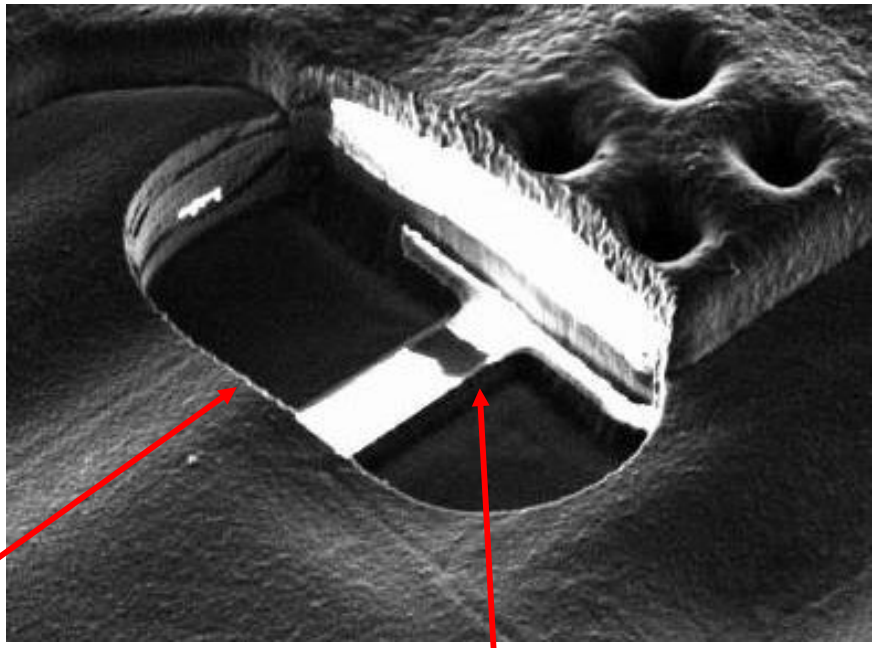
- use smaller circuitry
  - reducing size makes many physical attacks harder
- hide the bus
  - glue logic, and bus on lower layers of chip
- scramble bus lines
  - attacker has to optically reverse engineering this
- encrypting bus
- protective sensor mesh layer
  - to prevent access to chip surface
  - trend: accessing to chip surface from the back

Physical attack: probing

FIB = Focussed Ion Beam

can observe or modify chip by

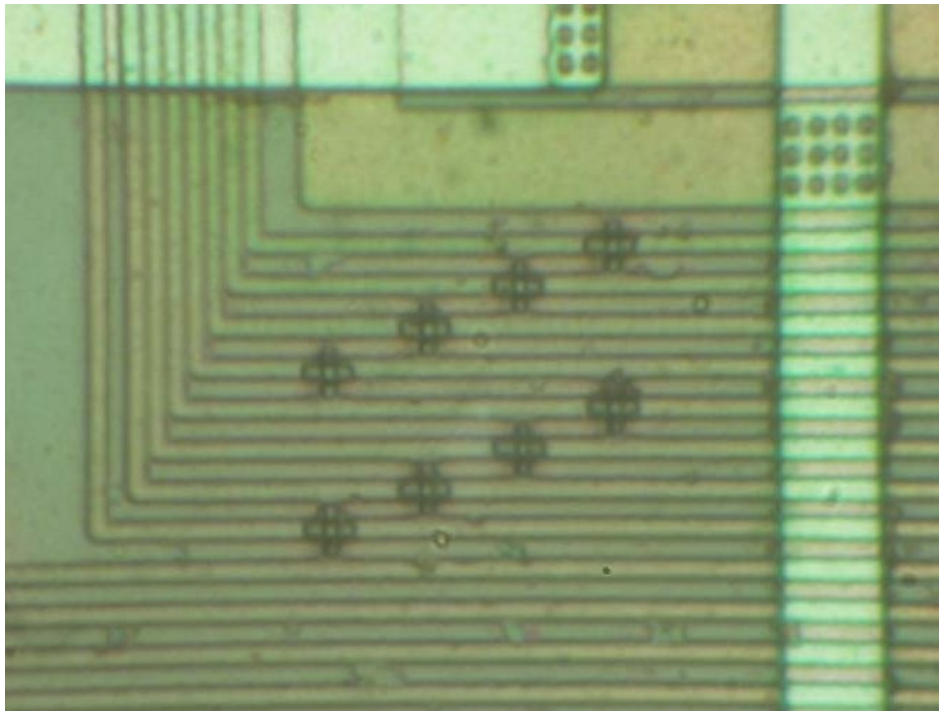
- drilling holes
- cutting connections
- soldering new connections and creating new gates



hole drilled in the chip surface

blown fuse

Using FIB in probing



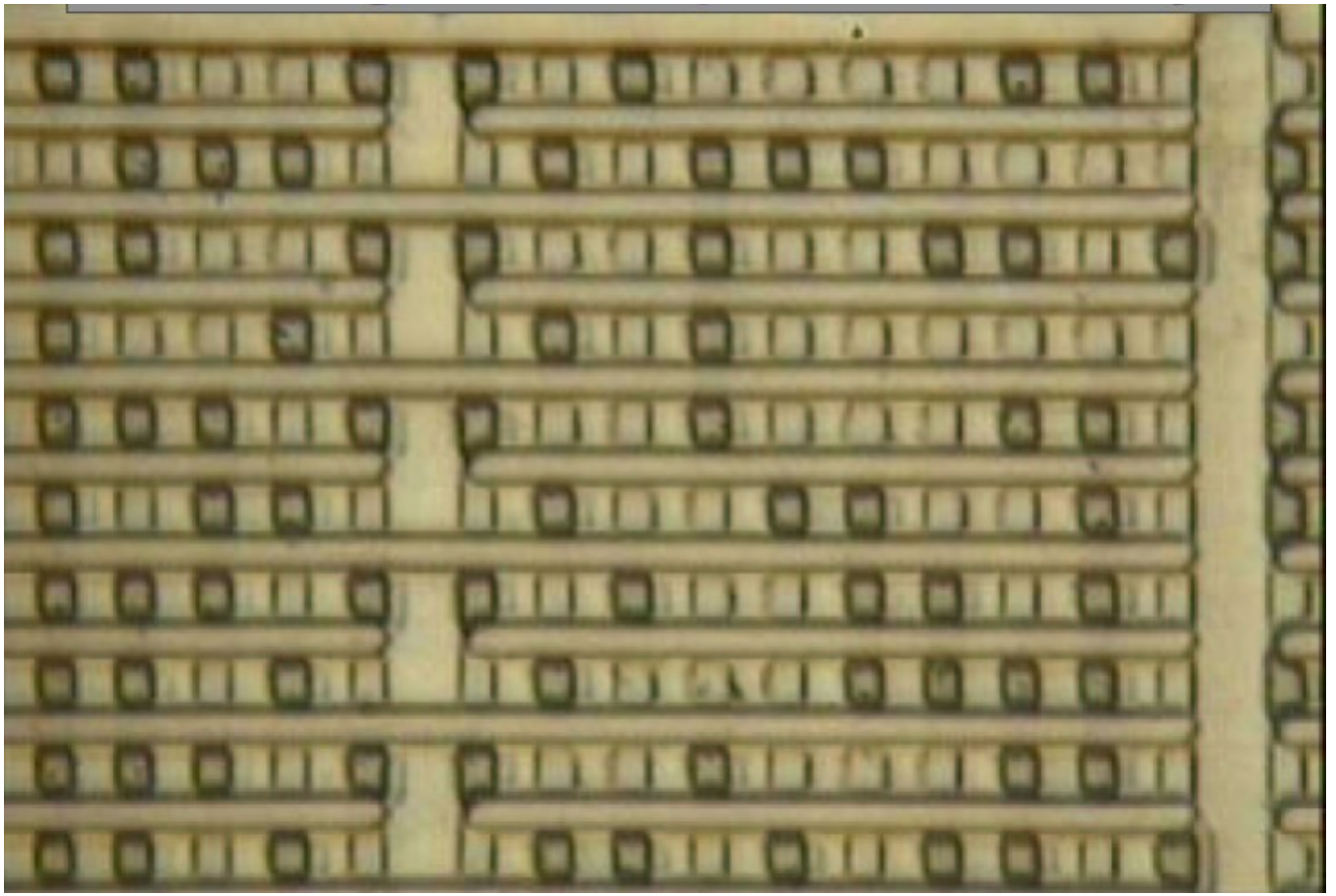
[Source: Sergei Skorobogatov]

Fibbing can be used to

- add probe pads for lines too thin or fragile for needles
- surface buried lines
  - poking holes through upper layers

Physical attack: extracting ROM content

Staining can optically reveal the bits stored in ROM:
dark squares are 1
light squares are 0



[Source: Brightsight]

Physical attack: extracting RAM content

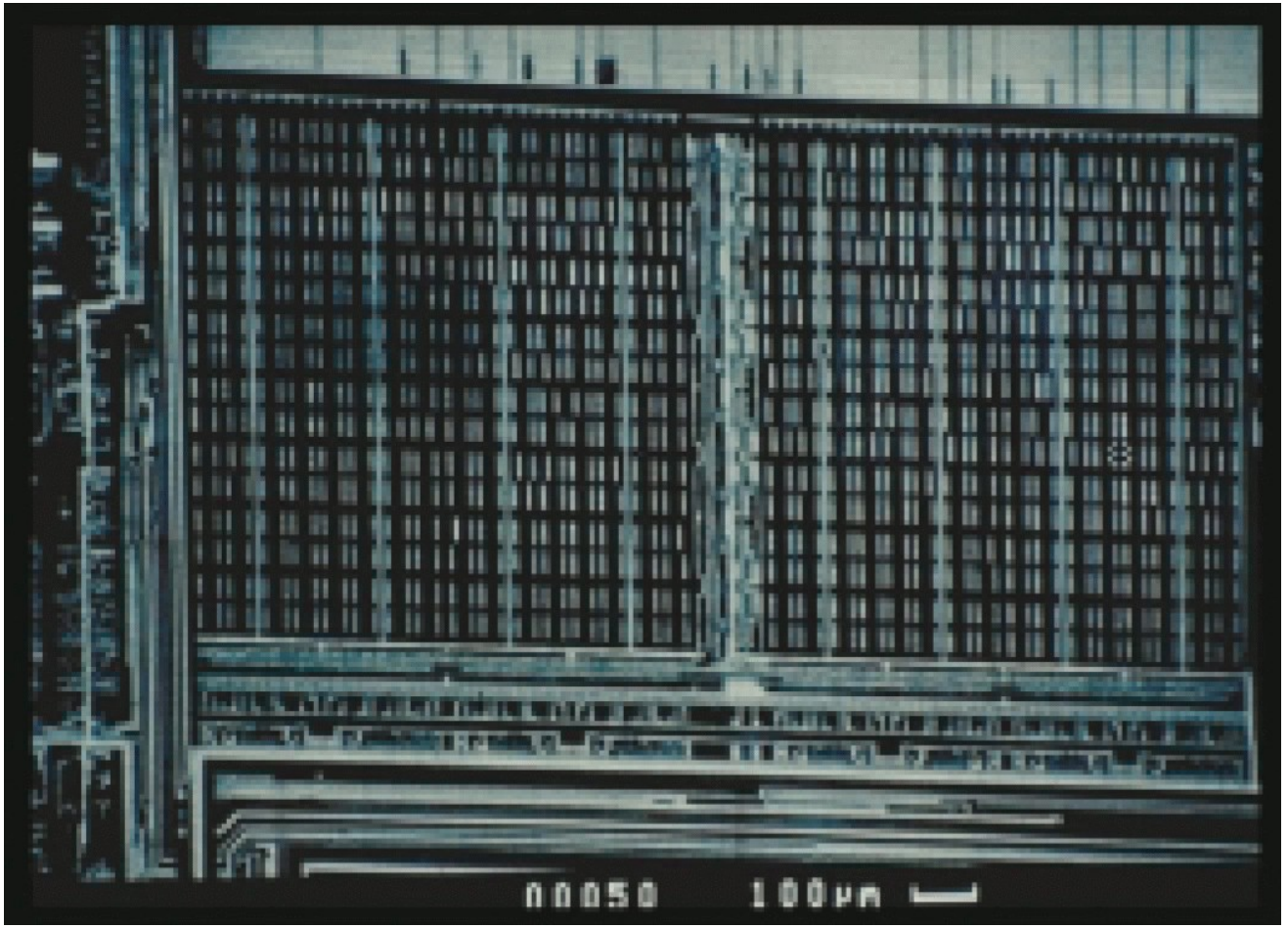


Image of RAM with voltage sensitive scanning electron microscope

memory extraction countermeasures

- obfuscate chip layout
- scramble or encrypt memo
- sensors
  - low and high temperatures, light, clock frequency, voltage, ...
  - But… external power supply is needed to react when intrusion is detected
  - Sensors can be destroyed when power is off => they must be tested periodically in normal operation

Conclusions

Why are smartcards everywhere?

- Cryptography provides a building block for security solutions, but also introduces security problems:
  1. key management & distribution
  2. who/what do we trust to *store* & *use* crypto keys?

Smartcards provide a possible solution

Conclusions

- Smartcards are a typical solution whenever more security than standard username/password login is needed.
- Smartcard security is not perfect!
  - it should not be the weakest link, in a well-designed system...
  - Smartcard is tamper-resistant and tamper-evident to certain degrees, but not tamper-proof
  - even if smartcard security is broken, there may be good measures for detection & reaction to limit impact
- The terminal problem is a serious limitation
  - More generally, we can secure connections between computers 1000's of miles apart, but not the last 2 feet from the computer and its human user.

Things can go wrong at many levels

- card itself, and the crypto, card configuration & protocols,, software
- terminals & terminal software
- organisational
  - issuance
  - usage

  incl. personnel, procedures, …

Issuance as the weakest link?

- You can obtain a new SIM for an existing number, claiming yours is broken or lost (or from a dodgy telecom provider, or insider?)
- Someone obtained a Dutch ID card with a picture of himself disguised as the Joker from Batman

More organisational hassle

- Issuing smartcards may be the easy part.

  Rolling out terminal equipment, dealing with organisation & training personnel may be the hard part

- *Eg for e-passports, introduced in the wake of 9/11:*
  - *few countries bother to read the chip on a regular basis*
  - *exchanging certificates (bilaterely via diplomatic post) is a big hassle*
  - *hardly any countries use fingerprint data*
    - *is quality of fingerprints info good enough ?*
    - *yet more certificate hassle, as terminal has to authenticate itself to passport with a terminal certificate*
  - *do personnel trust the chip, and can they interpret errors?*
  - *was it just security theatre?*
  - *or was the real motivation Automated Border Control?*

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations.

They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficently pervasive that we must design our protocols around their limitations

– Kaufman, Perlman, and Speciner