

Embedded Security



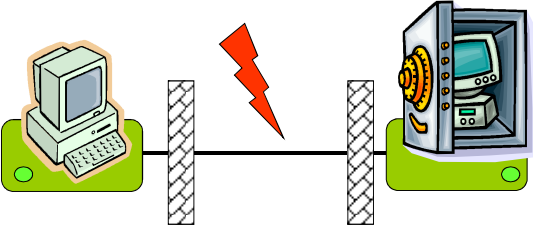
Benedikt Gierlichs
KU Leuven, COSIC

BalkanCryptSec 2014
Istanbul, Turkey

Acknowledgements:
Ingrid Verbauwhede, Patrick Schaumont, Kris Tiri,
Bart Preneel, Helena Handschuh



The Old Model (simplified view)



- Attack on channel between communicating parties
- Encryption and cryptographic operations in black boxes
- Protection by strong mathematic algorithms and protocols
- Computationally secure

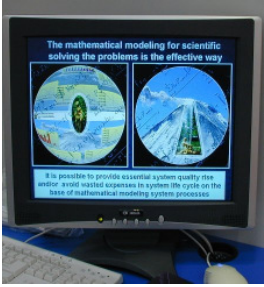
October 2014 BalkanCryptSec 2

Or so you think...


- Tempest: refers to investigations and studies of compromising emanations
 - Primarily: Electromagnetic radiation
 - Exploitation of signals and prevention
 - Term coined in the late 1960s (NSA)
 - Documents remain secret until today
 - Basic and redacted versions publicly available in the late 1990s
- Public research:
 - Van Eck phreaking (1985): reading computer screens from a "large" distance (also electronic voting machines)
 - Vuagnoux, Pasini (2009): keystroke logging from a distance (up to 20 meters), works on wireless and wired keyboards

October 2014 BalkanCryptSec 3

Screen reading from distance



← 25 meter →



<http://www.lightbluetouchpaper.org/2006/03/09/video-eavesdropping-demo-at-cebit-2006/>

October 2014 BalkanCryptSec 4

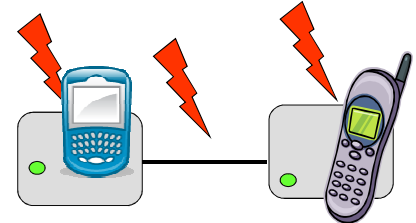
Embedded Cryptographic Devices



- A cryptographic device is an electronic device that implements a cryptographic algorithm and stores a cryptographic key. It is capable of performing cryptographic operations using that key.
- **Embedded:** it is exposed to adversaries in a hostile environment; full physical access, no time constraints
 - Note: the adversary might be a legitimate user!

October 2014 BalkanCryptSec 5

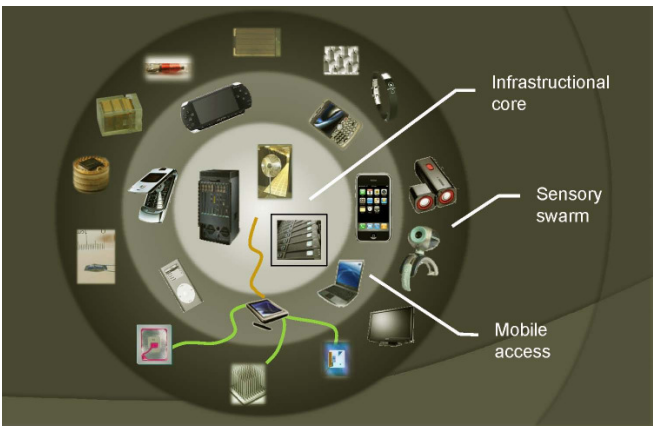
How is Embedded Security affected?



- New Model (also simplified view):
 - Attack on channel and endpoints
 - Encryption and cryptographic operations in gray boxes
 - Protection by strong mathematic algorithms and protocols
 - Protection by secure implementation
- **Need secure *implementations* not only algorithms**

October 2014 BalkanCryptSec 6

Internet of Things

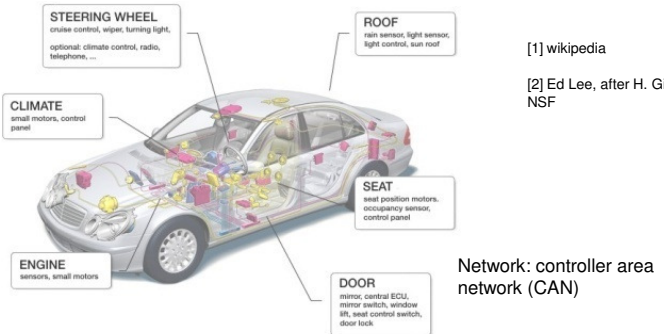


[Source photograph: J. Rabaey: A Brand New Wireless Day]

October 2014 BalkanCryptSec 7

Cyber physical systems

“A system of collaborating computational elements controlling physical entities” [1]
 “Networked embedded systems interacting with the environment” [2]



[1] wikipedia
 [2] Ed Lee, after H. Gill NSF

Network: controller area network (CAN)

October 2014 BalkanCryptSec 8

Medical devices, typical scenario

- Small embedded devices communicate over wireless link for sensing and actuation
- Goal: low energy (battery powered, temperature)
- Security goal: attack resistant

IMEC: Human++ project

October 2014 BalkanCryptSec 9

Interacting with the environment

Embedded crypto?

IMEC: NERF - brain stimulant

Deep Brain stimulation
[Sources: J. Rabaey, National Institutes of Health, Neurology journal]

October 2014 BalkanCryptSec 10

Always keep in mind

Your system is as secure as its weakest link

October 2014 BalkanCryptSec 11

Your system is as secure as its weakest link

Unknown source: seen on schneier.com

October 2014 BalkanCryptSec 12

Your system is as secure as its weakest link

And this house is even more secure! The front door is four feet thick and made of solid titanium...

Source: P. Kocher

October 2014 BalkanCryptSec 13

Your system is as secure as its weakest link

- The adversary will go for the weakest entry point
 - Disable or go around security mechanisms
 - Guess / spy on passwords
 - Bribe the security guard
- If you use **good** crypto, he will try to go around it
 - System designer: thinks of the "right" way to use the system
 - Adversary: does not play by the rules
- Designer has to think like the adversary, anticipate attacks, protect against them
- There is no way to protect against all attacks
 - Do you know all attacks?

October 2014 BalkanCryptSec 14

Security for Embedded Systems

"Researcher has a new attack for embedded devices
Vulnerability lies in ARM and XScale microprocessors"
Computerworld – security
April 4, 2007
How: Use JTAG interface

"Secustick gives false sense of security"
April 12, 2007
<http://tweakers.net/reviews/683>
Security completely broken

October 2014 BalkanCryptSec 15

Security for Embedded Systems

- SecuStick:
 - On plug-in: Windows program pops up and asks for password
 - Self-destructs if wrong password entered n-many times
- Attempt counter stored in flash memory chip
- Write-enable pin connected to GND: infinite number of attempts to guess the password ↴
- Password is checked in software routine on PC: changing return value from "0" to "1" gives full access ↴

April 12, 2007: <http://tweakers.net/reviews/683>

October 2014 BalkanCryptSec 16

Physical security of embedded cryptographic devices

- Let us assume that the system is well designed
 - Adversary cannot go around / disable security features
 - **Good** cryptography is used
- Embedded context, physical access
 - Adversary can "look" at the device under attack
 - Measure physical quantities
 - Adversary can manipulate the device under attack
 - Expose it to physical stress and "see" how it behaves

October 2014 BalkanCryptSec 17

Classification of Physical Attacks

- Active versus passive
 - Active: Perturbate and conclude
 - Passive: Observe and infer
- Invasive versus non-invasive
 - Invasive: open package and contact chip
 - Semi-invasive: open package, no contact
 - Non-invasive: no modification
- Side channel: passive and non-invasive
 - Very difficult to detect
 - Often cheap to set-up
 - Often: need lots of measurements automating
- Circuit modification: active and invasive
 - Expensive to detect invasion (chip might be without power)
 - Very expensive equipment and expertise required

October 2014 BalkanCryptSec 18

Side-Channel Leakage

- Physical attacks ≠ Cryptanalysis
(gray box, physics) (black box, maths)
- Does not tackle the algorithm's math. security

- Observe physical quantities in the device's vicinity and use additional information during cryptanalysis

October 2014 BalkanCryptSec 19

Some Side-Channels (not exhaustive)

- Timing
 - Overall or "local" execution time
- Power, Electromagnetic radiation
 - Predominant: CMOS technology
 - Consumes power when it does something, transistors switch
 - Electric current induces and EM field
- More exotic but shown to be practical
 - Light, Sound, Temperature

October 2014 BalkanCryptSec 20

Examples: measurement setups

- Smart cards
- FPGA, ASIC
- Phone, tablet
- Set-top boxes
- Etc.

source: langer-emv.de

October 2014 BalkanCryptSec 21

Side-Channel leakage

- Side-channel leakage
 - Is not intended
 - Information leakage was not considered at design time
 - Leaked information is not supposed to be known
 - Can enable new kind of attack
- Often, optimizations enable leakage
- Device under attack is operated in normal conditions
 - Adversary is passive and solely observes

October 2014 BalkanCryptSec 22

Principle is nothing new...

“Breaking into a Safe is hard, because one has to solve a single, very hard problem...”

“Divide et impera!”

“Things are different if it is possible to solve many small problems instead...”

October 2014 BalkanCryptSec 23

A timing attack

- 4-digit PIN verification
 - 10000 possible combinations
 - On average 5000 attempts necessary
 - Typically only 3 attempts allowed (counter)
 - Probability of correct guess: 3/10000

```

FUNCTION check (USER_PIN, CORRECT_PIN)
FOR i=1 TO PIN_LENGTH
    IF USER_PIN[i] != CORRECT_PIN[i]
        RETURN -1
ENDFOR
RETURN 0
    
```

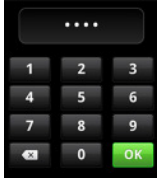
```

MAIN FUNCTION
...
IF check(...) == -1
    COUNTER++
ELSE
    COUNTER = 0
...
    
```

October 2014 BalkanCryptSec 24

A timing attack

- Execution time of *check(...)* leaks information



- o Test random PIN, measure time N
- o Change first PIN digit, measure time N'

 - o If $N == N'$ both digit guesses are wrong
 - o If $N > N'$ the first digit guess was correct
 - o If $N < N'$ the new digit guess is correct

- Average 5 (worst case 10) attempts per digit
- Average 20 (worst case 40) attempts per PIN
- ... but recall that only 3 attempts are allowed

October 2014
BalkanCryptSec
25

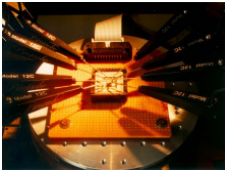
Concept of Side Channel attacks

- Some cryptographic algorithms gain their cryptographic strength by repeating a "weak" function many times
 - Classical model: adversary sees only final and secure result
- Other algorithms use few complex functions but their implementations follow a similar idea
- Side Channels leak information about these "weak" intermediate results
- Side Channel attacks exploit information about "weak" intermediate results

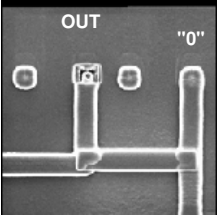
October 2014
BalkanCryptSec
26

Invasive attacks

- Passive: micro-probing
 - Probe the bus with a very thin needle
 - Read out data from bus or individual cells directly
 - Several needles concurrently
- Active: modify circuits
 - Connect or disconnect security mechanism
 - Disconnect security sensors
 - RNG stuck at a fixed value
 - Reconstruct blown fuses
 - Cut or paste tracks with laser or focused ion beam
 - Add probe pads on buried layers



[Helena Handschuh]



RNG

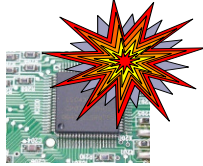
[www.fa-mal.com]

October 2014
BalkanCryptSec
27

Active attacks: fault injection

Apply combinations of strange environmental conditions

- Vcc
- Glitch
- Clock
- Temperature
- UV
- Light
- X-Rays
- ...



↑ ↓

input error

and bypass or infer secrets

Slide: Helena Handschuh

October 2014
BalkanCryptSec
28

Active attacks (semi invasive) fault injection

- Exploit faulty behavior provoked by physical stress applied to the device
- Semi-invasive: open package but no contact
 - Laser fault injection allows to target a relatively small surface area of the target device
 - Laser pulse frequency ~ 50Hz
 - Fully automated scan of chip surface
 - Once you have a weak spot: perturbate and exploit
 - Recent: 2 laser spots, 20 ns interval, diode lasers



[www.new-wave.com]

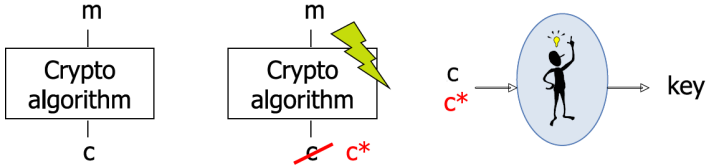
October 2014 BalkanCryptSec 29

Microscope view

October 2014 BalkanCryptSec 30

Differential Fault Analysis


- Ask for a cryptographic computation twice
 - With any input and no fault (reference)
 - With the same input and fault injection
- Infer information about the key from the output differential



- Sometimes a single fault injection is enough!

October 2014 BalkanCryptSec 31

Countermeasures



October 2014 BalkanCryptSec 32

Countermeasures: active and invasive attacks

- You cannot prevent the adversary from trying to mount an attack
- You can try to make it more difficult
 - "Hide" sensitive parts of the chip
 - Epoxy, metal layers, glue logic, etc.
- You can try to detect an attack and raise an alarm
 - Security sensors
 - Power, clock, light, temperature, wire mesh
 - Perform error check before outputting the result
 - Add redundancy, e.g. compute twice and compare
- Reaction to alarm: depends on security policy
 - Stop computing, reset, erase memory, self-destruct
 - Security vs usability

October 2014 BalkanCryptSec 33

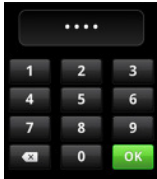
Countermeasures: passive and non-invasive attacks

- Very difficult (impossible?) to detect an attack!
 - Countermeasures always active
- Try to eliminate side channels, reduce information leakage, turn leaked information useless
 - Execution time independent of secret values
 - Sequence of operations independent of secret values
 - Randomization of data (masking)
 - Randomization of operation order (shuffling, random delays)
 - Decoupling and shielding
 - Balanced or masked logic
 -

October 2014 BalkanCryptSec 34

Back to the PIN example


- Assume the function *check(...)* runs in constant time



MAIN FUNCTION

```

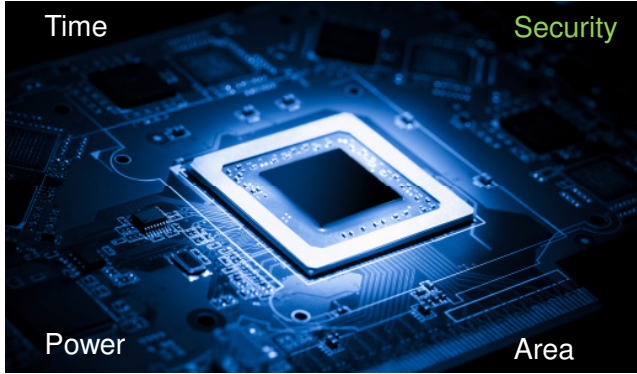
                ...
                IF check (...) == -1
                    COUNTER++
                ELSE
                    COUNTER = 0
                ...
            
```



- Attacker can target main function to get unlimited attempts
 - Disconnect power supply before increasing counter
 - "Skip" instructions using glitches
- Better: increase, check, decrease (defensive programming)

October 2014 BalkanCryptSec 35

Embedded security requirements



[wonderfulengineering.com]

October 2014 BalkanCryptSec 36

Security as a design dimension

- Security consumes resources!
 - extra area, extra power, extra time, development overhead
 - E.g. communication – computation trade-off
- *Similar* to power or area optimization
 - Perfect security does not exist (zero-power design doesn't exist either)
 - Low-risk security does exist (low-power design does exist)
- *Different*: attacker will go for the easiest entry point:
 - If strong crypto algorithm: try other weaknesses
 - Monitor power consumption, electromagnetic radiation, timing
 - Introduce glitches (= fault attacks)
 - Guess the password
 - Bribe the security guard (= social engineering)

October 2014

BalkanCryptSec

37

Thank you for your attention!



October 2014

BalkanCryptSec

38