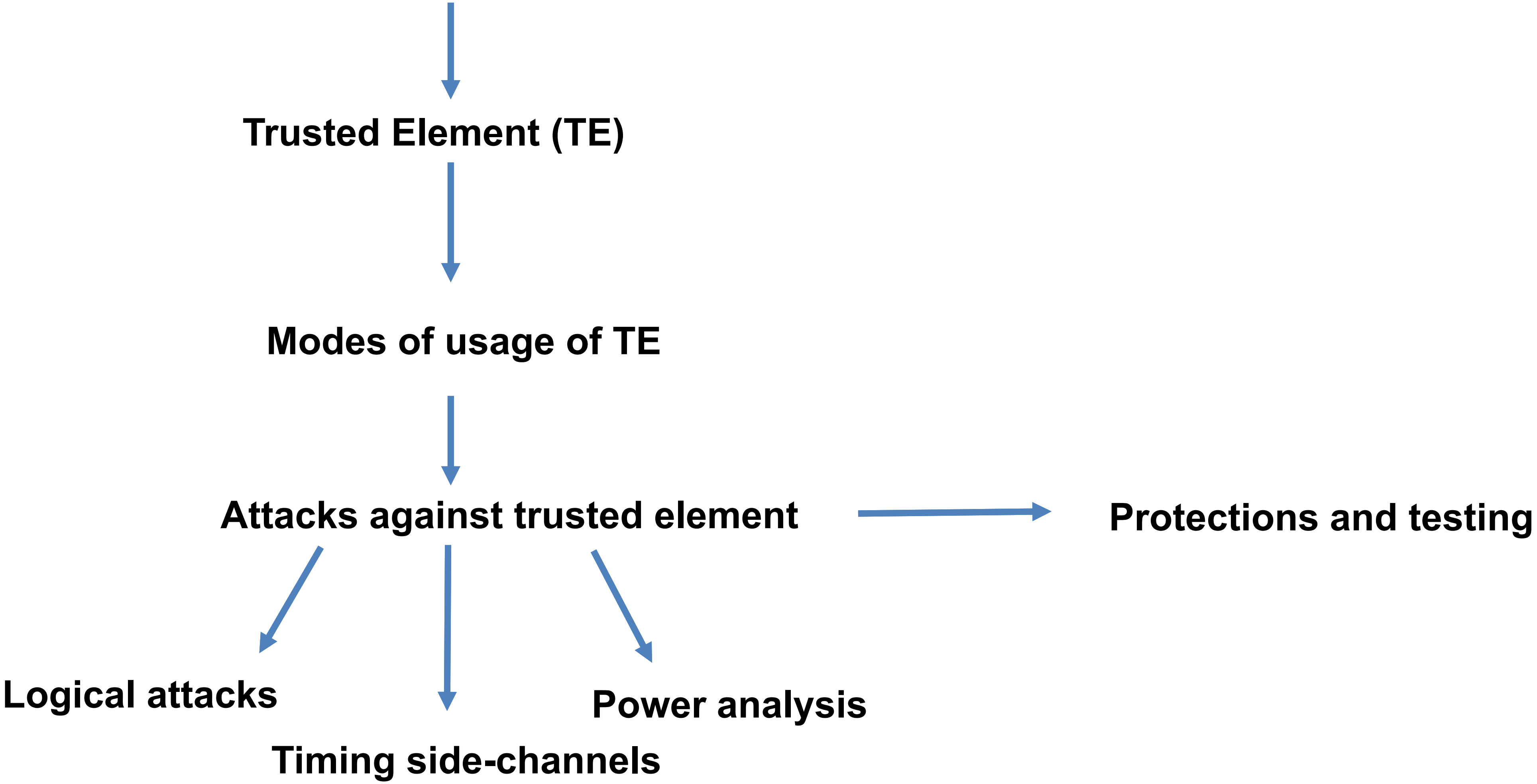
PV204 Security technologies

Trust, trusted element, usage scenarios, side-channel attacks

Petr Švenda ✉ *svenda@fi.muni.cz* *@rngsec*
Centre for Research on Cryptography and Security, Masaryk University

CRoCS
Centre for Research on
Cryptography and Security

What is untrusted, trusted and trustworthy



Trusted Element (TE)

Modes of usage of TE

Attacks against trusted element

Protections and testing

Logical attacks

Timing side-channels

Power analysis

- Group activity: Make trusted trustworthy
  - Took almost 20 minutes
  - Moderately interesting, but good opportunity to discuss nuances during answers collection
- Lecture ended before Example: Remote extraction OpenSSL RSA slide
- ROCA was covered only briefly

TRUSTED ELEMENT

What is “Trusted” system (plain language)

- Many different notions

1. System trusted by someone
2. System that you can’t verify and therefore must trust not to betray you
   - If a trusted component fails, security can be violated
3. System build according to rigorous criteria so you are willing to trust it
4. …

- Why Trust is Bad for Security, D. Gollman, 2006
  - http://www.sciencedirect.com/science/journal/15710661/157/3

We need more precise specification of Trust

UNTRUSTED VS. TRUSTED VS. TRUSTWORTHY

Untrusted system

- System itself explicitly unable to fulfill specified security policy
- Additional layer of protection must be employed
  - E.g., Encryption of data before storage
  - E.g., Digital signature of email before send over network
  - E.g., End-to-end encryption in instant messaging

Trusted system

- *"…system that is relied upon to a specified extent to enforce a specified security policy. As such, a trusted system is one whose failure may break a specified security policy."* (TCSEC, Orange Book)
- Trusted subjects are those excepted from mandatory security policies (Bell LaPadula model)
- User must trust (if wants to use the system)
  - E.g., you and your bank

Trustworthy system (computer)

- *"Computer system where software, hardware, and procedures are secure, available and functional and adhere to security practices"* (Black's Law Dict.)
- User have reasons to trust reasonably
- Trustworthiness is subjective
  - Limited interface and hardware protections can increase trustworthiness (e.g., append-only log server)
- Example: Payment card - Trusted? Trustworthy?

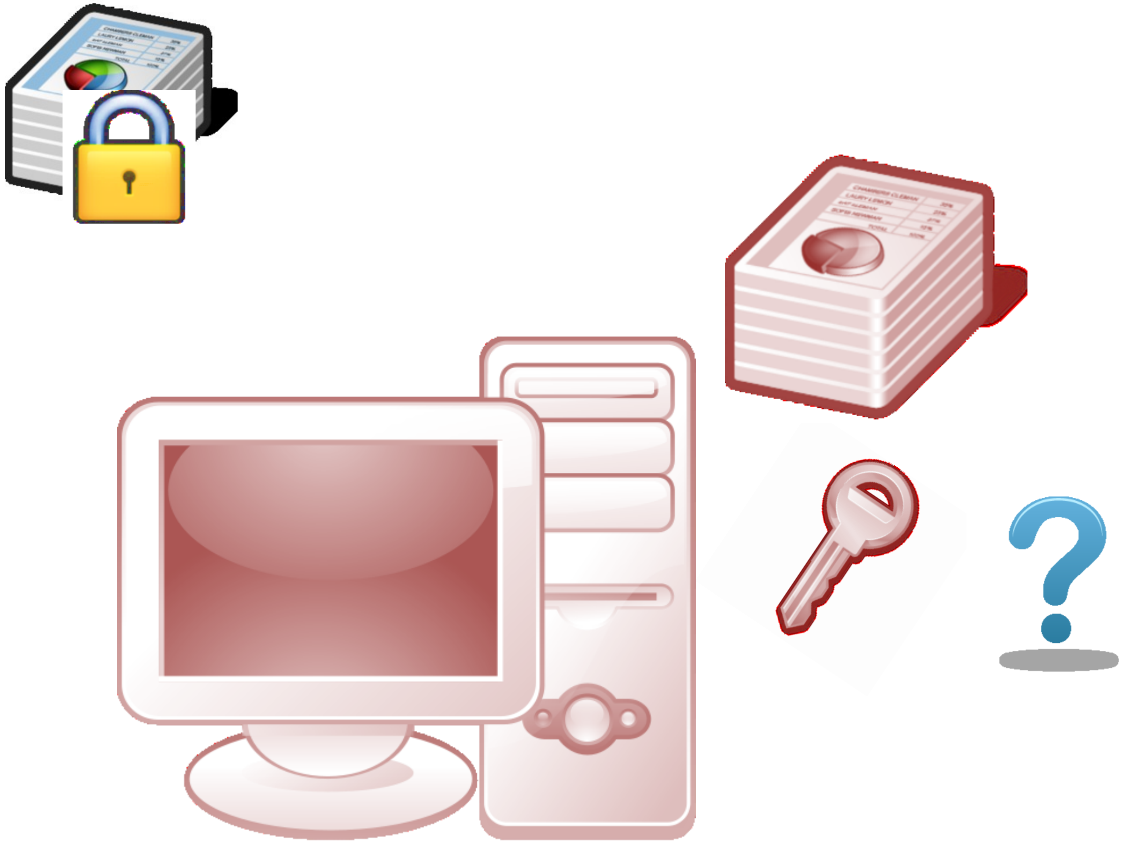
Trusted does not mean automatically *Trustworthy*

Trusted computing base (TCB)

- The set of all hardware, firmware, and/or software components that are critical to its security
- The vulnerabilities inside TCB might breach the security properties of the entire system
  - E.g., server hardware + virtualization (VM) software
- The boundary of TCB is relevant to usage scenario
  - TCB for datacentre admin is around HW + VM (to protect against compromise of underlying hardware and services)
  - TCB for web server client also contains Apache web server
- Very important factor is size and attack surface of TCB
  - Bigger size implies more space for bugs and vulnerabilities

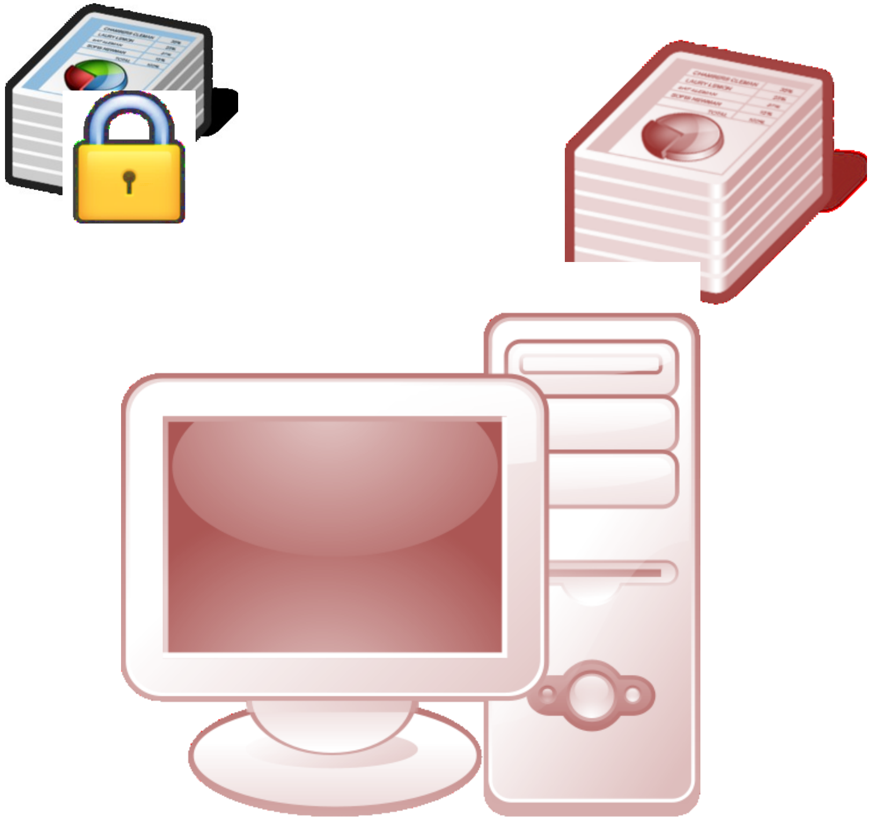
https://en.wikipedia.org/wiki/Trusted_computing_base

Cryptography on client

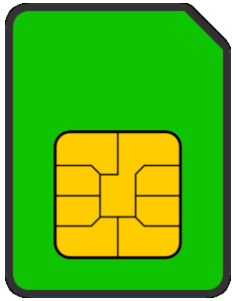


Which parts are trusted?
What are threats?
What are attacker models?
What is trusted computing base?

On client, but with secure hardware



Which parts are trusted?
What are threats?
What are attacker models?
What is trusted computing base?



Group activity: Make trusted trustworthy

- Write 2 different examples of trusted system you regularly use
- Write down why exactly it needs to be trusted and with what operations
- (5 minutes)

- Pick one system and propose 3 changes to make it more trustworthy
- (5 minutes)

- Combine results found by groups

TRUSTED ELEMENT

What exactly can be trusted element (TE)?

- Recall: Anything user entity of TE is willing to trust ☺
  - Depends on definition of “trust” and definition of “element”
  - We will use narrower definition
- Trusted element is element (hardware, software or both) in the system intended to increase security *level* w.r.t. situation without the presence of such element
  1. By storage of sensitive information (keys, measured values)
  2. By enforcing integrity of execution of operation (firmware update)
  3. By performing computation with confidential data (DRM)
  4. By providing unforged reporting from untrusted environment (TPM)
  5. …

Typical examples

- Payment smart card
  - TE for issuing bank
- SIM card
  - TE for phone carriers
- Trusted Platform Module (TPM)
  - TE for user as storage of Bitlocker keys, TE for remote entity during attestation
- Trusted Execution Environment in mobile/set-top box
  - TE for issuer for confidentiality and integrity of code
- Hardware Security Module for TLS keys
  - TE for web admin
- Energy meter
  - TE for utility company
- Server under control of service provider
  - TE for user – private data, TE for provider – business operation

For whom is TE trusted?

Risk management

- No system is completely secure (→ risk is present)
- Risk management allows to evaluate and eventually take additional protection measures
- Example: payment transaction limit
  - “My account/card will never be compromised” vs. “Even if compromised, the loss is bounded”
- Example: medical database
  - central governmental DB vs. doctor’s local DB

💡 Good design practice is to allow for risk management

TRUSTED ELEMENT MODES OF USAGE

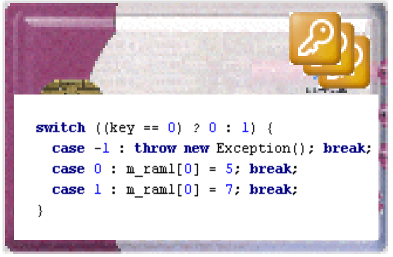
Trusted (hardware) element - modes of usage

1. Element carries fixed information

2. Element as a secure carrier

3. Element as encryption/signing device

4. Element as programmable device



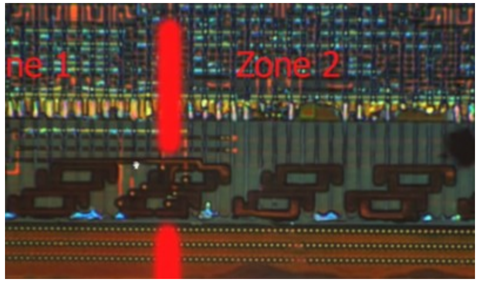
```
switch ((key == 0) ? 0 : 1) {
  case -1 : throw new Exception(); break;
  case 0 : m_ram1[0] = 5; break;
  case 1 : m_ram1[0] = 7; break;
}
```

5. Element as root of trust (TPM)

Is secure hardware trusted element a silver bullet?

1. Trusted element shall be small (TCB) => Not whole system => How to extend desirable security properties from TE to whole system?
2. The trusted element itself can still be directly attacked

Trusted hardware (TE) is not panacea!



1. Can be physically attacked
   - Christopher Tarnovsky, BlackHat 2010
   - Infineon SLE 66 CL PE TPM chip, bus read by tiny probes
   - 9 months to carry the attack, $200k
   - https://youtu.be/w7PT0nrK2BE (great video with details)
2. Attacked via vulnerable API implementation
   - IBM 4758 HSM (Export long key under short DES one)
3. Provides trusted anchor != trustworthy system
   - Weakness can be introduced later
   - E.g., bug in newly updated firmware

Motivation: Bell’s Model 131-B2 / Sigaba

- Encryption device intended for US army, 1943
  - Oscilloscope patterns detected during usage
  - 75 % of plaintexts intercepted from 80 feets
  - Protection devised (security perimeter), but forgot after the war
- CIA in 1951 – recovery over ¼ mile of power lines
- Other countries also discovered the issue
  - Russia, Japan…
- More research in use of (eavesdropping) and defense against (shielding) → TEMPEST

Common and realizable attacks on Trusted Element

1. Non-invasive attacks
   - API-level attacks
     - Incorrectly designed and implemented application
     - Malfunctioning application (code bug, faulty generator)
   - Communication-level attacks
     - Observation and manipulation of communication channel
   - Side-channel attacks
     - Timing/power/EM/acoustic/cache-usage/error… analysis attacks
2. Semi-invasive attacks
   - Fault induction attacks (power/light/clock glitches…)
3. Invasive attacks
   - Dismantle chip, microprobes…

How to reason about attack and countermeasures?

1. Where does an attack come from (principle)?
   – Understand the principles
2. Different hypothesis for the attack to be practical
   – More ways how to exploit the same weakness
3. Attack’s countermeasures by cancel of hypothesis
   – For every way you are aware of
4. Costs and benefits of the countermeasures
   – Cost of the assets protected
   – Cost for an attacker to perform attack
   – Cost of a countermeasure

Important: Consider Break Once, Run Everywhere (BORE)

Where are the frequent problems with crypto algs nowadays?

- Security mathematical algorithms
  - OK, we have very strong ones (AES, SHA-3, RSA…) (but quantum computers)
- Implementation of algorithm
  - Problems → implementation attacks
- Randomness for keys
  - Problems → achievable brute-force attacks
- Key distribution
  - Problems → old keys, untrusted keys, key leakage
- Operation security
  - Problems → where we are using crypto, key leakage

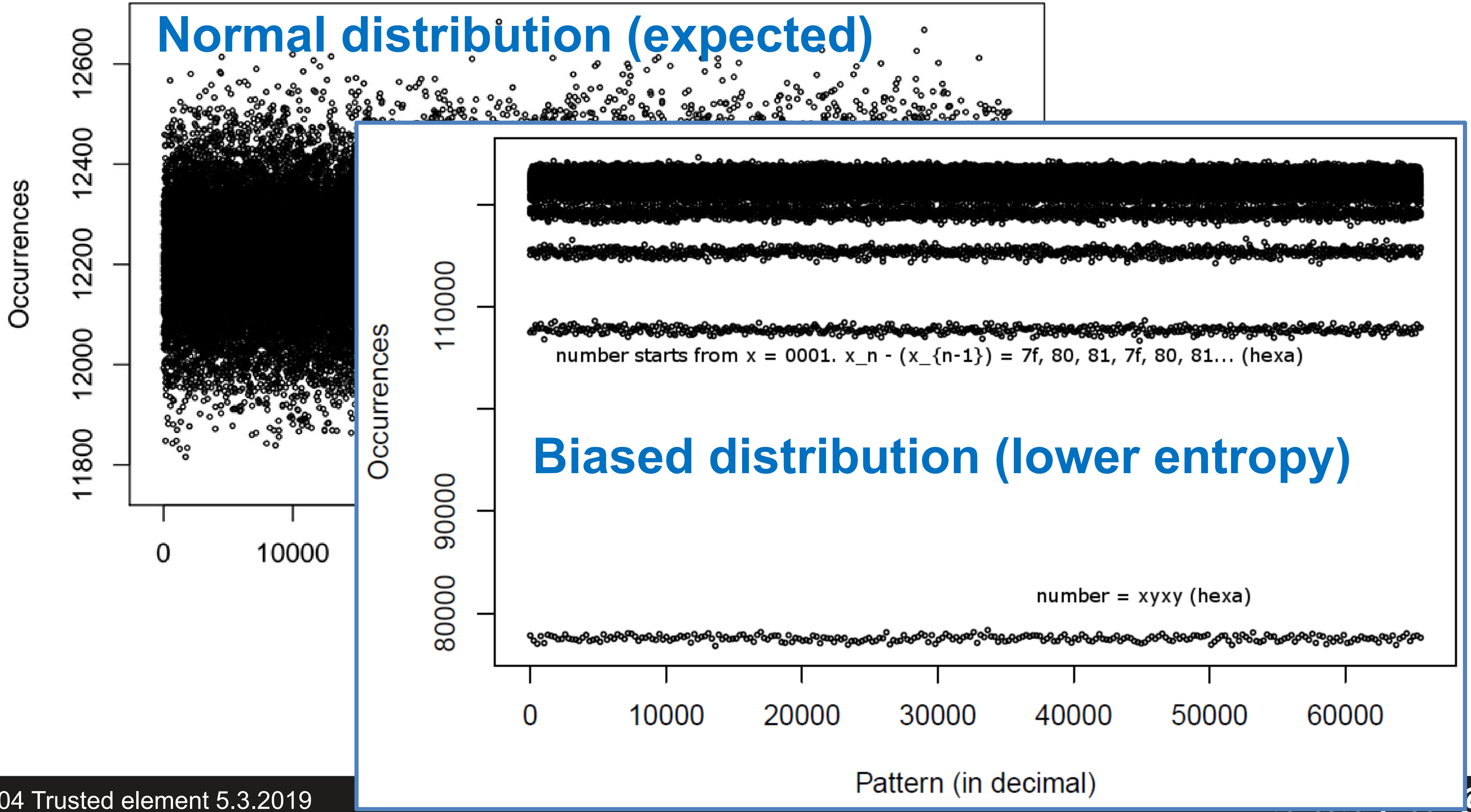
Non-invasive attacks

NON-INVASIVE LOGICAL ATTACKS

What if faulty Truly Random Number Generator (TRNG)?

- Good source of randomness is critical
  - TRNG can be weak or malfunctioning
- How to inspect TRNG correctness?
  1. Analysis of TRNG implementation (but usually blackbox)
  2. Output data can be statistically tested (100MB-8GB stream, NIST STS, Dieharder, TestU01 batteries) http://www.phy.duke.edu/~rgb/General/dieharder.php
  3. Behaviour in extreme condition (+70/-50° C, radiation…)
     - Analyse data stream gathered during extreme conditions
  4. Simple power analysis of TRNG generation
     - Is hidden/unknown operation present?

Serial test: Histogram of 16bits patterns



Normal distribution (expected)

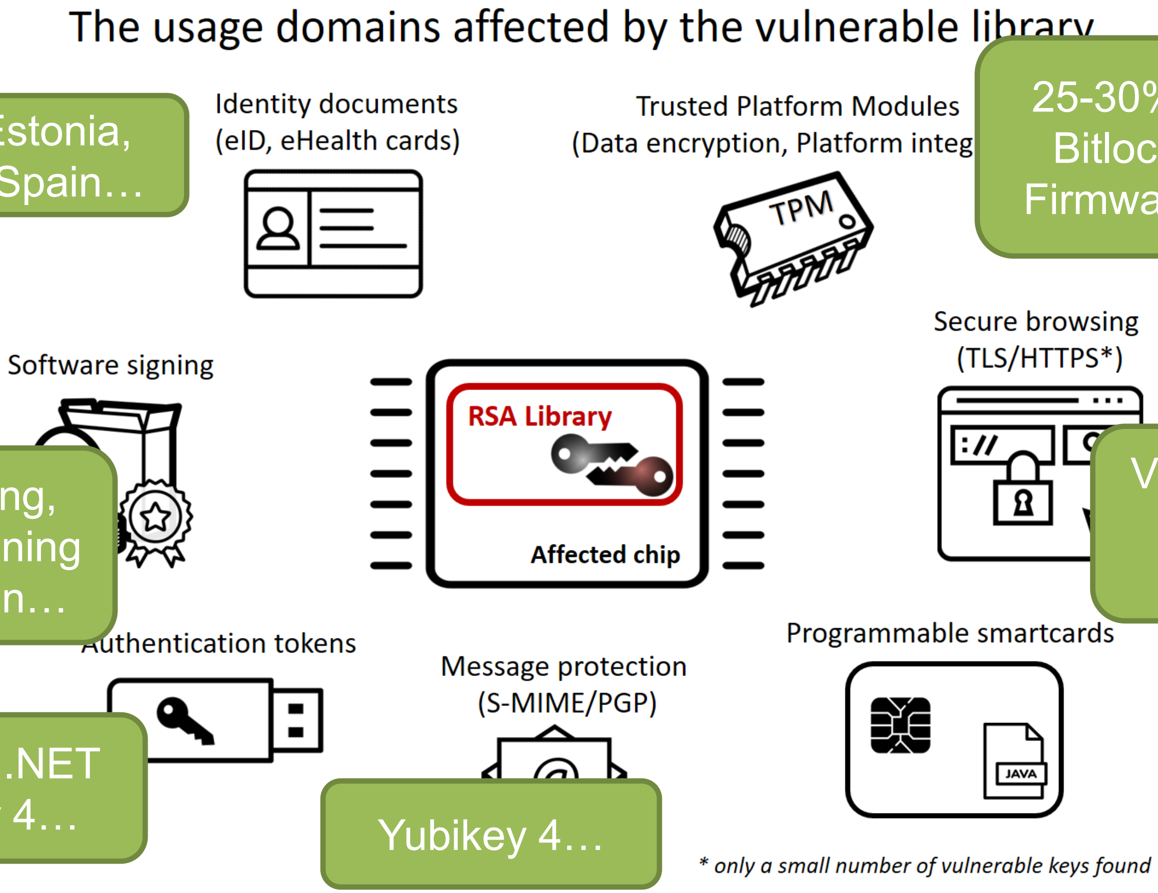
Biased distribution (lower entropy)

number starts from x = 0001. x_n - (x_{n-1}) = 7f, 80, 81, 7f, 80, 81... (hexa)

number = xyxy (hexa)

Algorithmic flaw in Infineon’s RSALib (CVE-2017-15361)

M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas: The Return of Coppersmith’s Attack..., ACM CCS 2017


The usage domains affected by the vulnerable library
Identity documents (eID, eHealth cards)
Trusted Platform Modules (Data encryption, Platform integ
TPM
Software signing
RSA Library
Affected chip
Secure browsing (TLS/HTTPS*)
://
Authentication tokens
Message protection (S-MIME/PGP)
Programmable smartcards
JAVA
* only a small number of vulnerable keys found

Austria, Estonia, Slovakia, Spain…

25-30% TPMs worldwide, Bitlocker, ChromeOS… Firmware update available

Commit signing, Application signing GitHub, Maven…

Very few keys, but all tied to SCADA management

Gemalto .NET Yubikey 4…

Yubikey 4…

Flawed use of random data to make primes

$$N = p * q$$

$$p_{ideal} = \text{random prime}$$

$$p_{Infineon} = (k * M + 65537^{a} \bmod M);\ \ a, k \in \mathbb{Z}$$

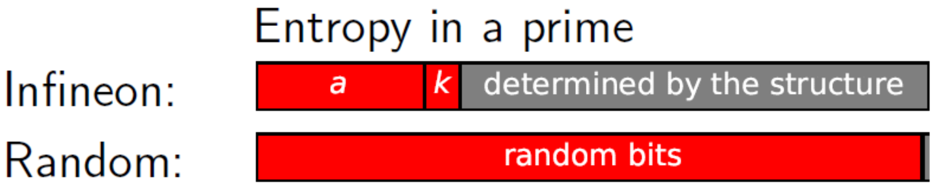
$$M = 2 * 3 * 5 * 7 * \cdots * P_n$$

Special structure of primes to facilitate its faster generation

~310 bits of entropy for 1024-bit prime

Consequences of the structure:

1. Fingerprint
2. Entropy loss
3. Factorization is possible

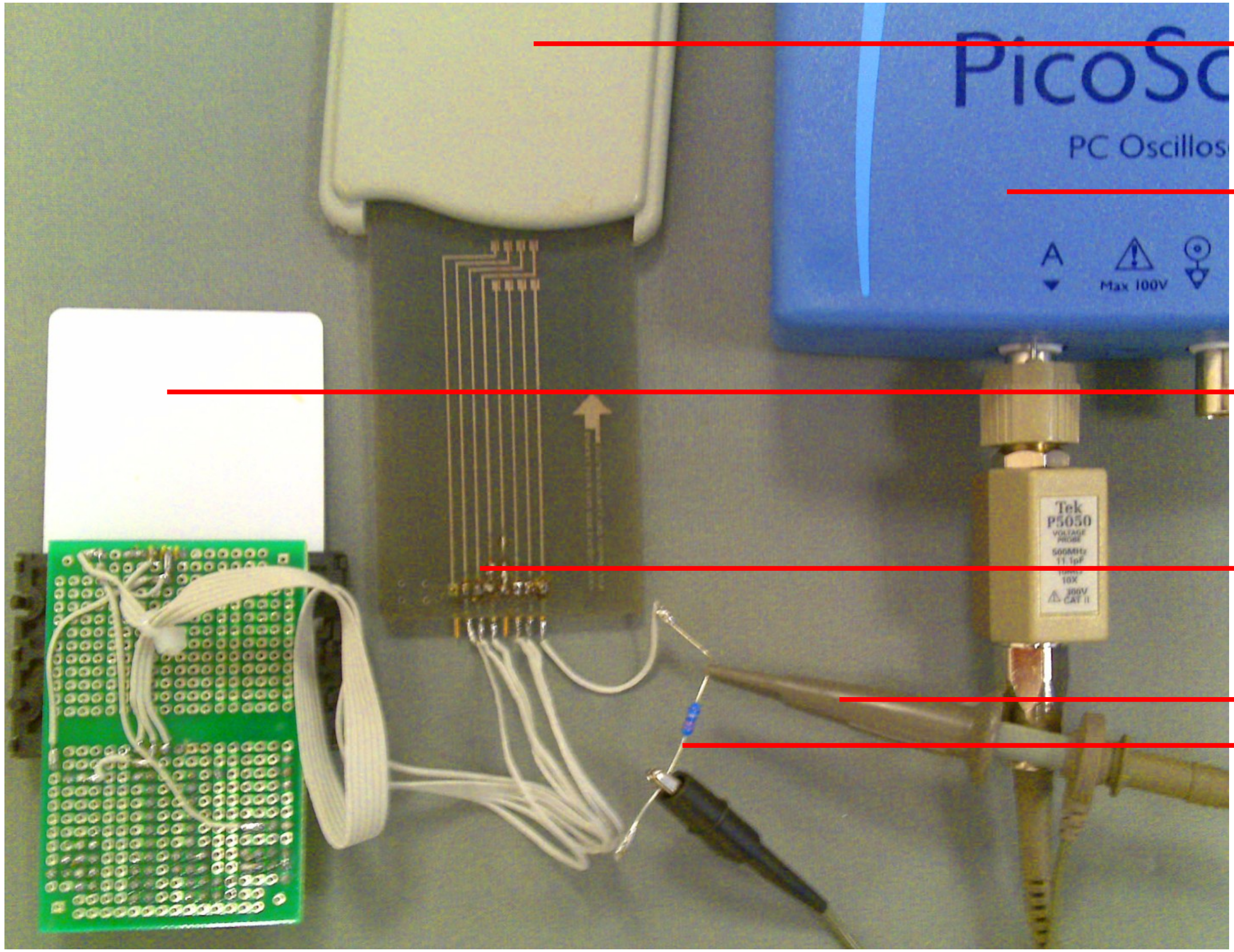


- Factorization difficulty
  - Random 2048b key: 6442450944000000 vCPU years
  - Infineon 2048b key: 140 vCPU years

Non-invasive side-channel attacks

POWER ANALYSIS

Basic setup for power analysis



Smart card reader

Oscilloscope

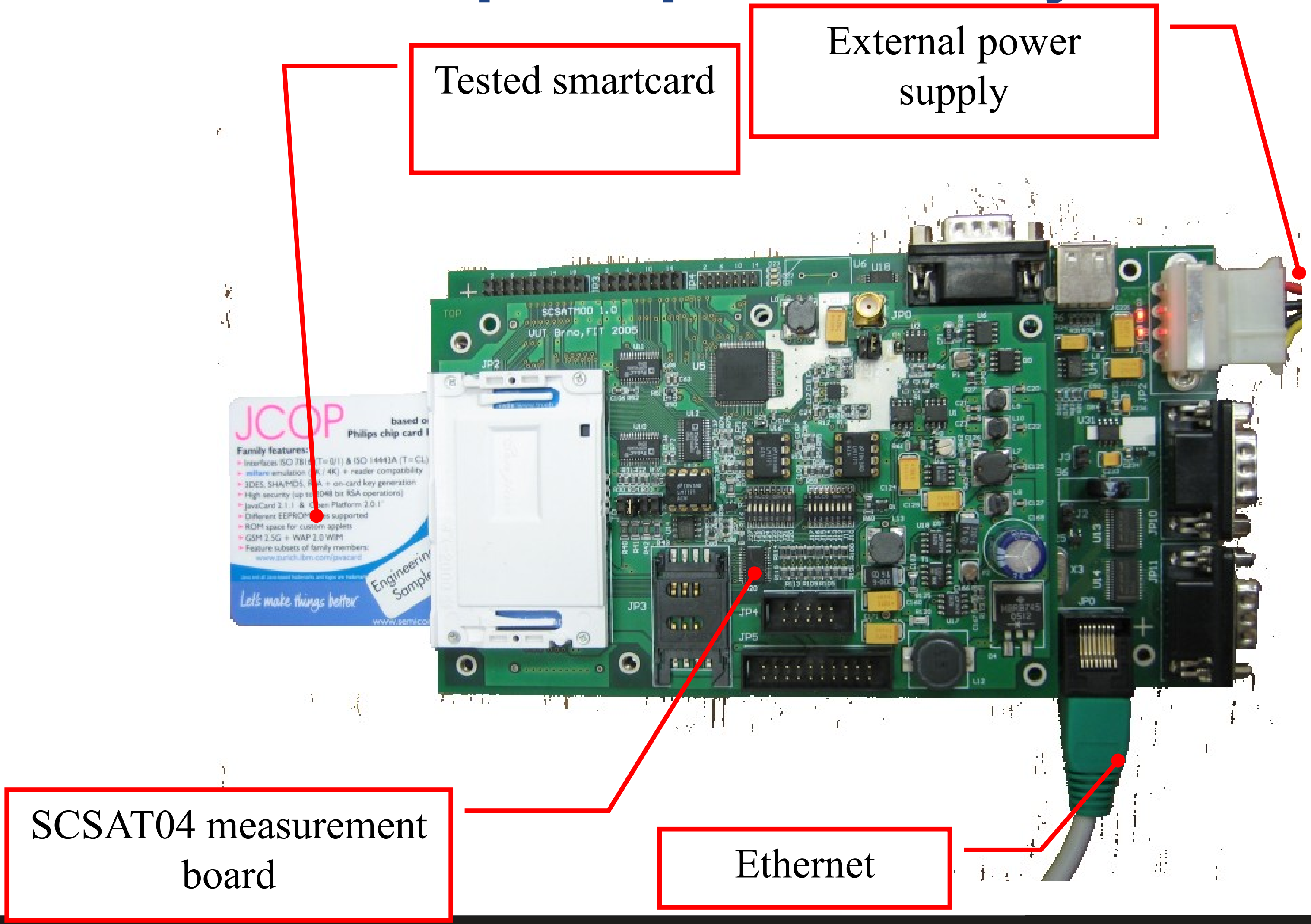
Smart card

Inverse card connector

Probe

Resistor 20-80 ohm

More advanced setup for power analysis



Tested smartcard

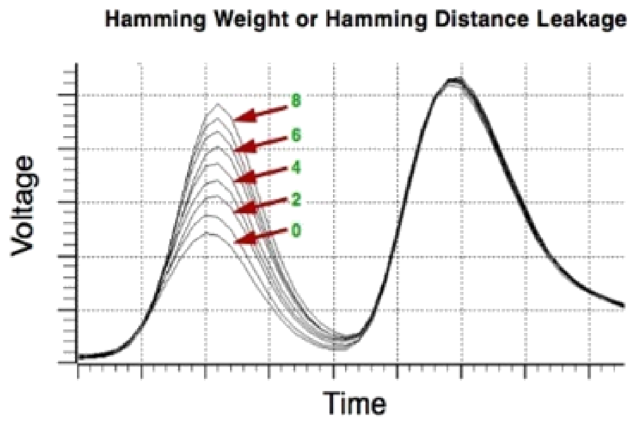
External power supply

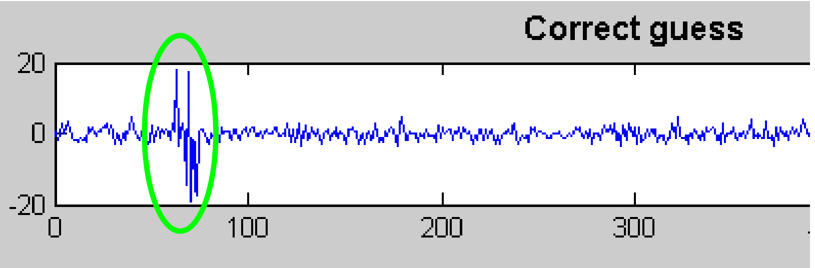
SCSAT04 measurement board

Ethernet

Simple vs. differential power analysis

1. Simple power analysis
   - Direct observation of single / few power traces
   - Visible operation => reverse engineering
   - Visible patterns => data dependency
2. Differential power analysis
   - Statistical processing of many power traces
   - More subtle data dependencies found





Reverse engineering of JavaCard bytecode

- Goal: obtain code back from smart card
  - JavaCard defines around 140 bytecode instructions
  - JVM fetch instruction and execute it

(source code)

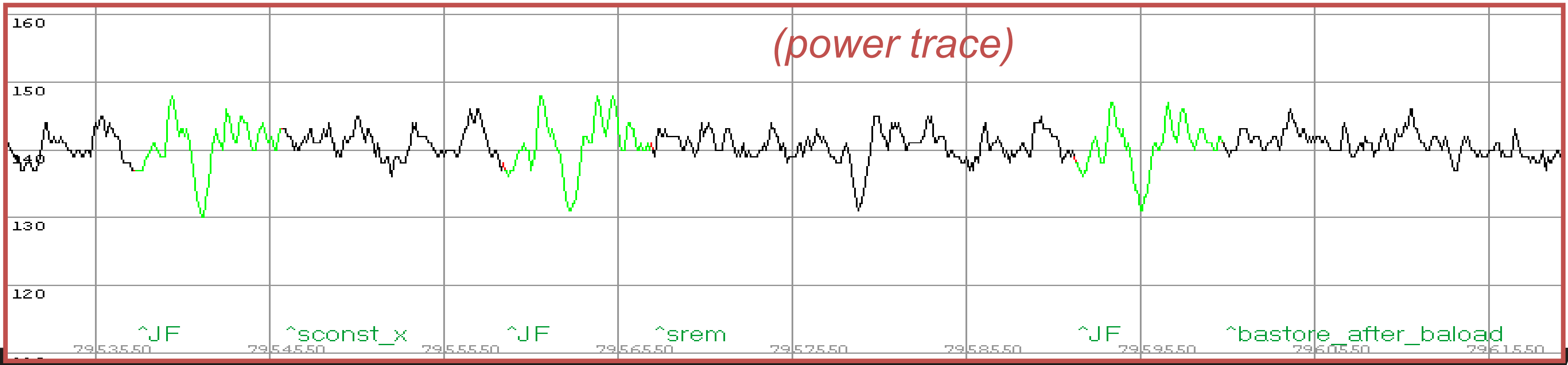
```
m_ram1[0] = (byte) (m_ram1[0] % 1);
```

compiler →

(bytecode)

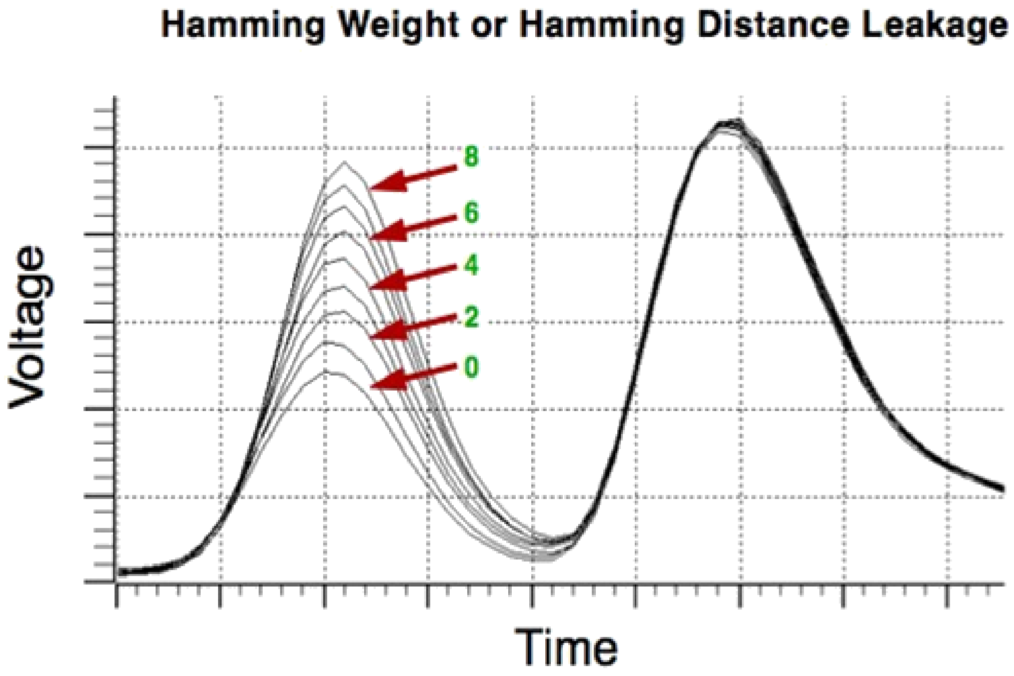
```
getfield_a_this 0;
sconst_0;
baload;
sconst_1;
srem;
bastore;
```

oscilloscope →



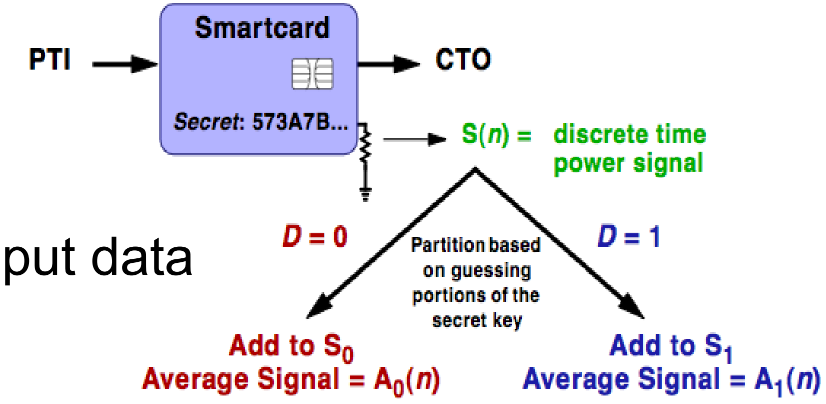
Simple power analysis – data leakage

- Data revealed directly when processed
  - e.g., Hamming weight of instruction argument
    - hamming weight of separate bytes of key ($2^{56} \rightarrow 2^{38}$)



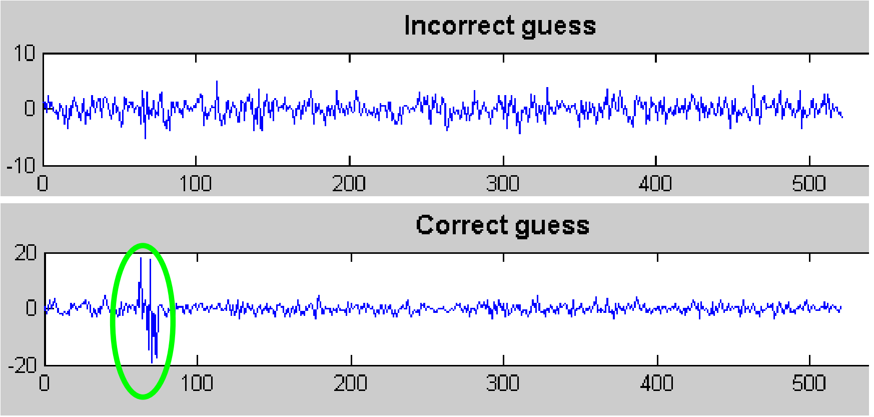
Differential power analysis (DPA)

- DPA attack recovers secret key (e.g., AES)
- Requires large number of power traces (10^2-10^6)
  - Every trace measured on AES key invocation with different input data
- Key recovered iteratively
  - One recovered byte at the time ($KEY_i \oplus INPUT\_DATA_i$)
  - Guess possible key byte value (0-255), group measurements, compute average, determine match



PTI
Smartcard
Secret: 573A7B...
CTO
S(n) = discrete time power signal
D = 0
Partition based on guessing portions of the secret key
D = 1
Add to S_0
Average Signal = $A_0(n)$
Add to S_1
Average Signal = $A_1(n)$

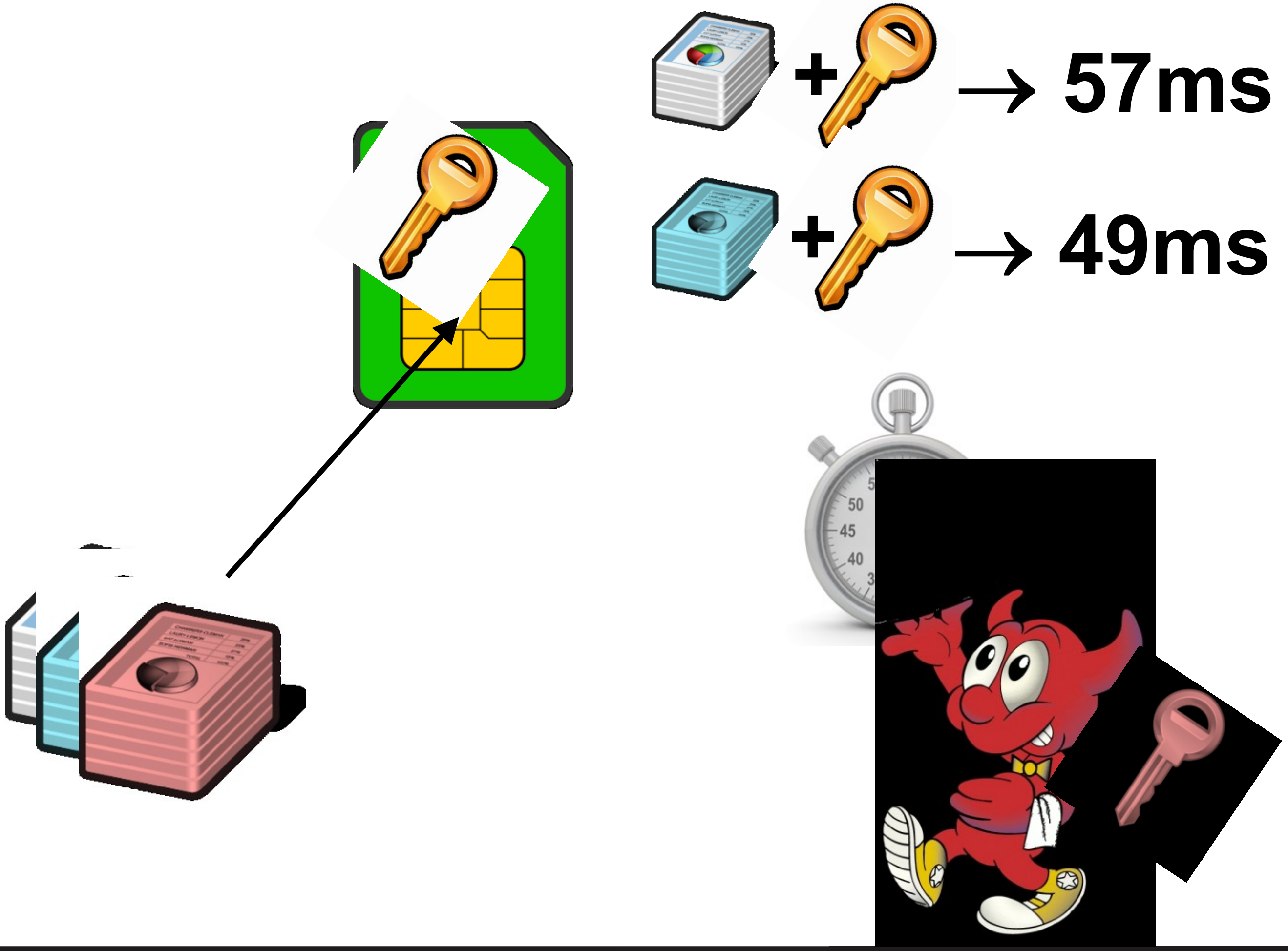
Define: DPA Bias Signal = $T(n) = A_1(n) - A_0(n)$



Non-invasive side-channel attacks

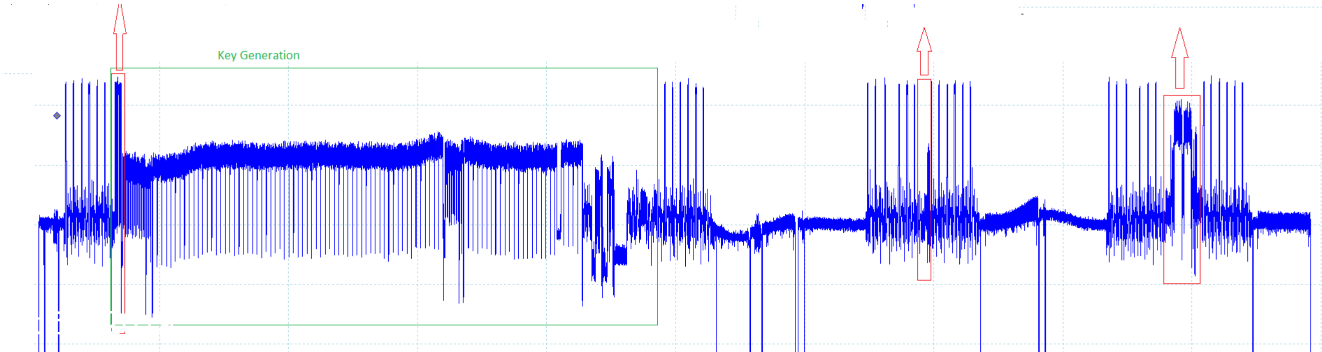
TIMING ATTACKS

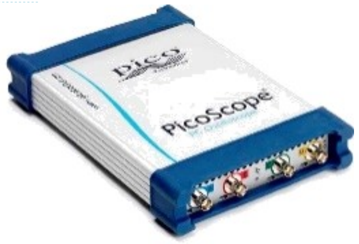
Timing attack: principle



Timing attacks

- Execution of crypto algorithm takes different time to process input data with some dependence on secret value (secret/private key, secret operations…)
  1. Due to performance optimizations (developer, compiler)
  2. Due to conditional statements (branching)
  3. Due to cache misses
  4. Due to operations taking different number of CPU cycles
- Measurement techniques
  1. Start/stop time (aggregated time, local/remote measurement)
  2. Power/EM trace (very precise if operation can be located)





Naïve modular exponentiation (modexp) (RSA/DH…)

- $M = C^d \bmod N$

Is there any dependency of time on secret value?

- $M = \overbrace{C * C * C * \ldots * C}^{\text{d-times}} \bmod N$

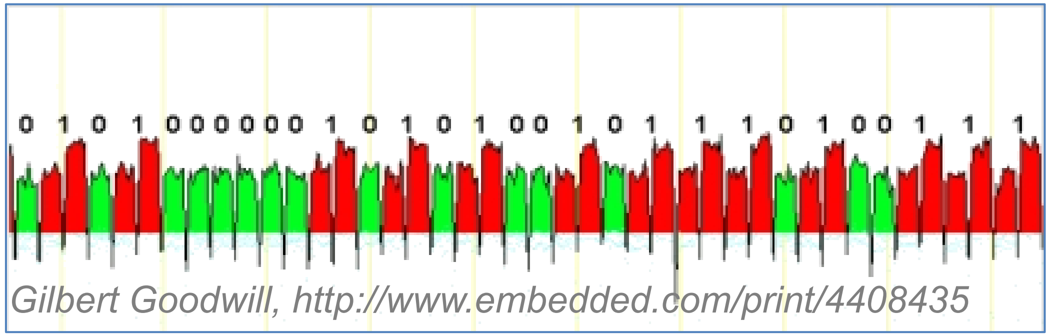
- Easy, but extremely slow for large d (e.g., >1000s bits for RSA)
  – Faster algorithms exist

Faster modexp: Square and multiply algorithm

Executed always

Executed only when d_j == 1

```
// M = C^d mod N
// Square and multiply algorithm
x = C                         // start with ciphertext
for j = 1 to n {              // process all bits of private exponent
    x = x*x mod N             // shift to next bit by x * x (always)
    if (d_j == 1) {           // j-th bit of private exponent d
      x = x*C mod N           // if 1 then multiple by Ciphertext
    }
}
return x        // plaintext M
```



Gilbert Goodwill, http://www.embedded.com/print/4408435

- How to measure?
  - Exact detection from simple power trace
  - Extraction from overall time of multiple measurements

Faster and more secure modexp: Montgomery ladder

- Computes x^d mod N
- Create binary expansion of d as $d = (d_{k-1} \ldots d_0)$ with $d_{k-1}=1$

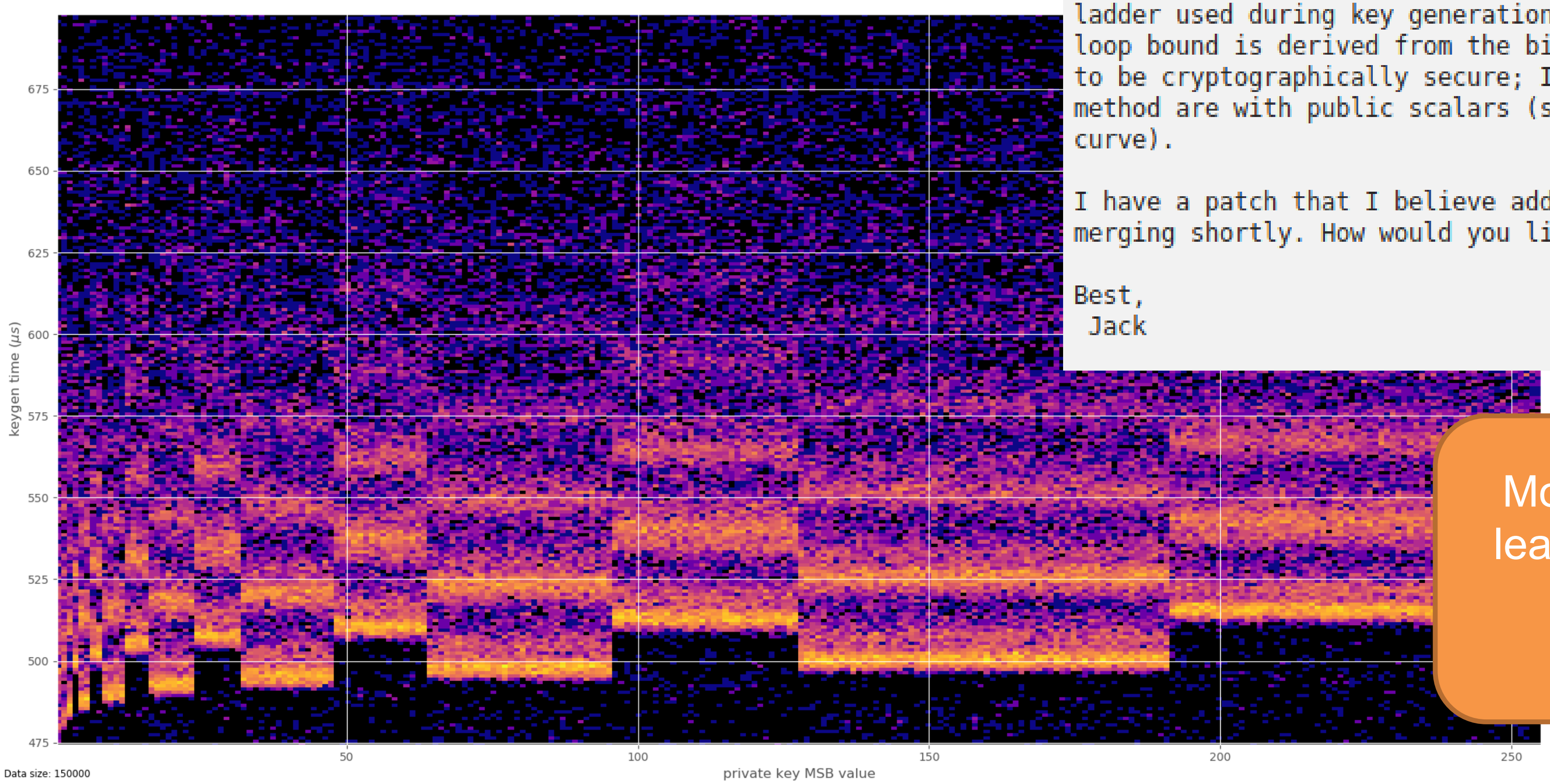
```
$x_1=x$; $x_2=x^2$
for j=k-2 to 0 {
  if $d_j=0$
    $x_2=x_1*x_2$; $x_1=x_1^2$
  else
    $x_1=x_1*x_2$; $x_2=x_2^2$
  $x_2=x_2$ mod N
  $x_1=x_1$ mod N
}
return $x_1$
```

Both branches with the same number and type of operations (not unlike square and multiply on previous slide)

- Be aware: timing leakage still possible via cache side channel, non-constant time CPU instructions, variable k-1…

Example: Botan library, ECC, CVE-2018-20187 (Jan Jančár)

Heatmap of private key MSBs to keygen time



```
Hi Ján,

Thank you for the report. I believe you are correct, the Montgomery
ladder used during key generation leaks the size of the scalar as the
loop bound is derived from the bit length. That function was not meant
to be cryptographically secure; I checked and all other uses of this
method are with public scalars (such as the cofactor or order of the
curve).

I have a patch that I believe addresses the problem which I will be
merging shortly. How would you like this to be credited in the release notes?

Best,
 Jack
```

Montgomery ladder used, but leakage of exponent size via k

for j=k-2 to 0 **do**

Example: Remote extraction OpenSSL RSA

- Brumley, Boneh, Remote timing attacks are practical
  - https://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf
- Scenario: OpenSSL-based TLS with RSA on remote server
  - Local network, but multiple routers
  - Attacker submits multiple ciphertexts and observe processing time (client)
- OpenSSL's RSA CRT implementation
  - Square and multiply with sliding windows exponentiation
  - Modular multiplication in every step: x*y mod q (Montgomery alg.)
  - From timing can be said if normal or Karatsuba was used
    - If x and y has unequal size, normal multiplication is used (slower)
    - If x and y has equal size, Karatsuba multiplication is used (faster)
- Attacker learns bits of prime by adaptively chosen ciphertexts
  - About 300k queries needed

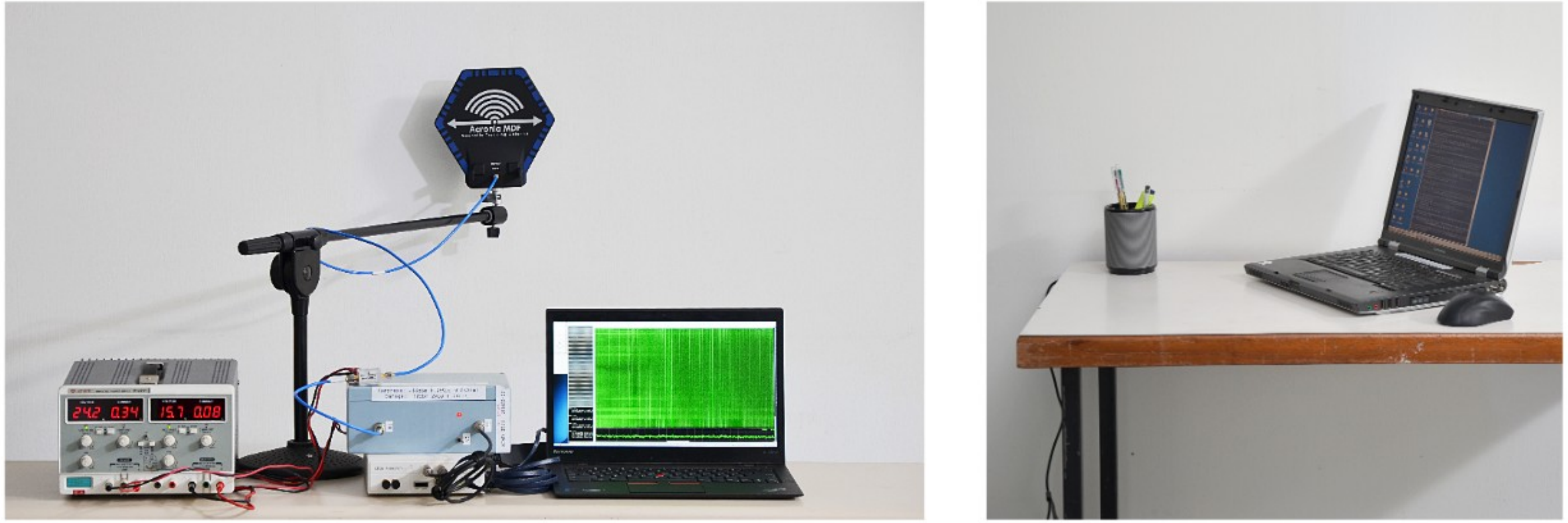
Defense introduced by OpenSSL

- RSA blinding: RSA_blinding_on()
  - https://www.openssl.org/news/secadv_20030317.txt
- Decryption without protection: M = c^d mod N
- Blinding of ciphertext *c* before decryption
  1. Generate random value *r* and compute r^e mod N
  2. Compute blinded ciphertext *b* = *c* * r^e *mod N*
  3. Decrypt *b* and then divide result by *r*
     - *r* is removed and only decrypted plaintext remains

$$(r^e \cdot c)^d \cdot r^{-1} \mod n = r^{ed} \cdot r^{-1} \cdot c^d \mod n = r \cdot r^{-1} \cdot c^d \mod n = m.$$

Example: Practical TEMPEST for $3000

- ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs
  - https://eprint.iacr.org/2016/129.pdf
- E-M trace captured (across a wall)

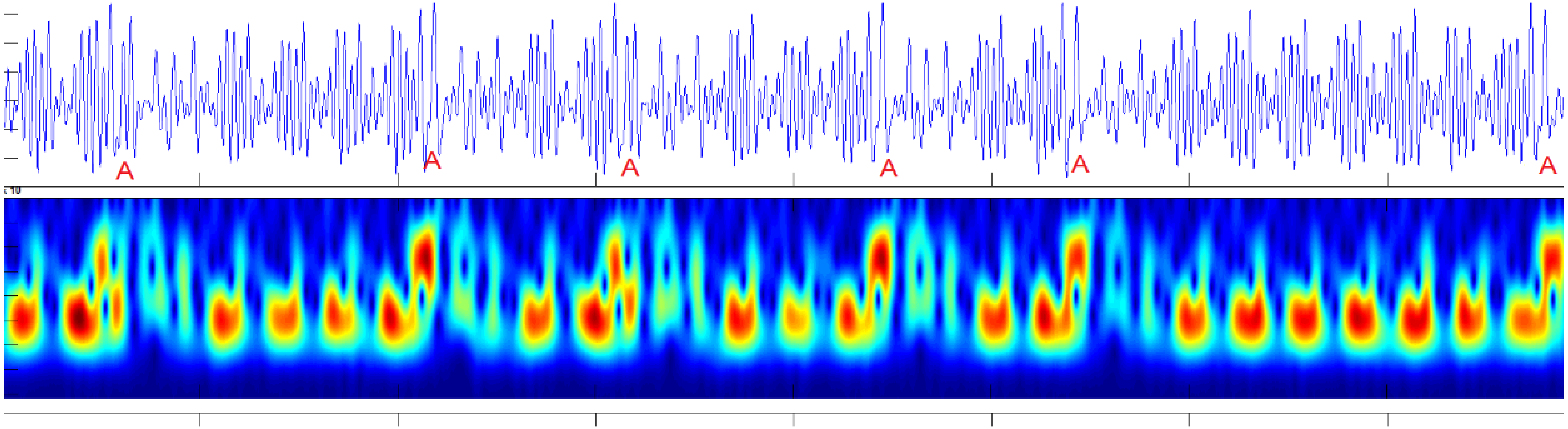


(a) Attacker's setup for capturing EM emanations. Left to right: power supply, antenna on a stand, amplifiers, software defined radio (white box), analysis computer.

(b) Target (Lenovo 3000 N200), performing ECDH decryption operations, on the other side of the wall.

Example: Practical TEMPEST for $3000

- ECDH implemented in latest GnuPG's Libgcrypt
- Single chosen ciphertext – used operands directly visible

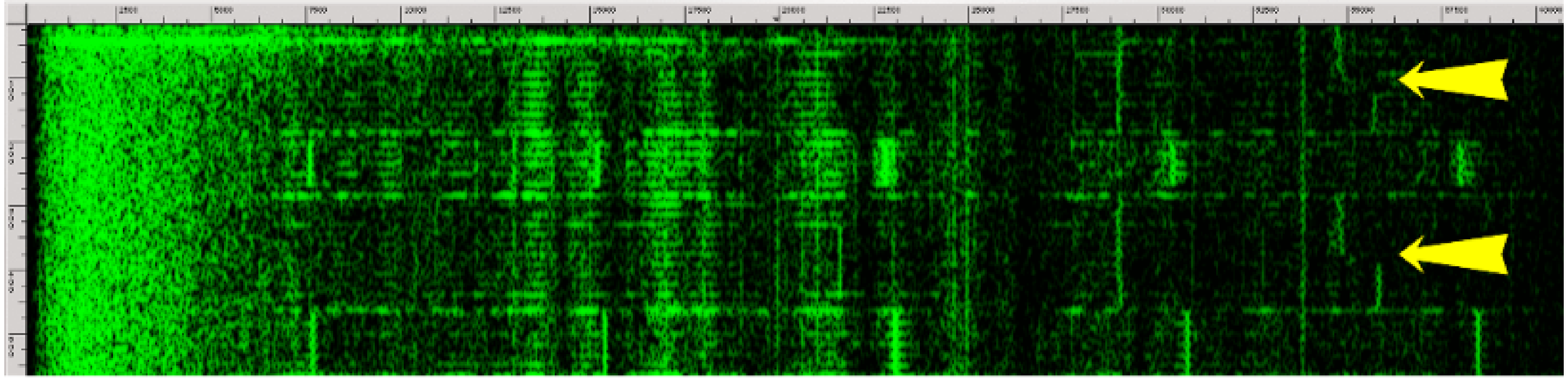


Example: How to evaluate attack severity?

- What was the cost?
  - Not particularly high: $3000
- What was the targeted implementation?
  - Widely used implementation: latest GnuPG's Libgcrypt
- What were preconditions?
  - Physical presence, but behind the wall
- Is it possible to mitigate the attack?
  - Yes: fix in library, physical shielding of device, perimeter…
  - What is the cost of mitigation?

Example: Acoustic side channel in GnuPG

- RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis
  - Insecure RSA computation in GnuPG
  - https://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf
- Acoustic emanation used as side-channel
  - 4096-bit key extracted in one hour
  - Acoustic signal picked by mobile phone microphone 4 meters away



Example: Cache-timing attack on AES

- Attacks not limited to asymmetric cryptography
  - Daniel J. Bernstein, http://cr.yp.to/antiforgery/cachetiming-20050414.pdf
- Scenario: Operation with secret AES key on remote server
  - Key retrieved based on response time variations of table lookups cache hits/misses
  - 2^{25} x 600B random packets + 2^{27} x 400B + one minute brute-force search
- Very difficult to write high-speed but constant-time AES
  - Problem: table lookups are not constant-time
  - Not recognized / required by NIST during AES competition

- Cache-time attacks now more relevant due to processes co-location (cloud)

Other types of side-channel attacks

- Acoustic emanation
  - Keyboard clicks, capacitor noise
  - Speech eavesdropping based on high-speed camera
- Cache-occupation side-channel
  - Cache miss has impact on duration of operation
  - Other process can measure own cache hits/misses if cache is shared
- Branch prediction side-channel (Meltdown, Spectre)

MITIGATIONS

Generic protection techniques

1. Shielding - preventing leakage outside
   - Acoustic shielding, noisy environment
2. Creating additional “noise”
   - Parallel software load, noisy power consumption circuits
3. Compensating for leakage
   - Perform inverse computation/storage
4. Harden algorithm
   - Ciphertext blinding…

Example: NaCl (“salt”) library

- Relatively new cryptographic library (2012)
  - Designed for usable security and side-channel resistance
  - D. Bernstein, T. Lange, P. Schwabe
  - https://cr.yp.to/highspeed/coolnacl-20120725.pdf
  - Actively developed fork is libsodium https://github.com/jedisct1/libsodium
- Designed for usable security (hard to misuse)
  - Fixed selection of good algorithms (AE: Poly1305, Sign: EC Curve25519)
  - `C = crypto_box(m,n,pk,sk), m = crypto_box_open(c,n,pk,sk)`
- Implemented to have constant-time execution
  - No data flow from secrets to load addresses
  - No data flow from secrets to branch conditions
  - No padding oracles (recall CBC padding oracle in PA193)
  - Centralizing randomness and avoiding unnecessary randomness

How to test real implementation?

1. Be aware of various side-channels
2. Obtain measurement for given side-channel
   - Many times (10^3 - 10^7), compute statistics
   - Same input data and key
   - Same key and different data
   - Different keys and same data…
3. Compare groups of measured data
   - Is difference visible? => potential leakage
   - Is distribution uniform? Is distribution normal?
4. Try to measure again with better precision ☺

Activity: Side-channels (10 minutes)

1. Power consumption of memory write instruction depends on the Hamming weight of stored byte
2. Time required to execute `inc` instruction (a++) is faster than `add` instruction (a+b)
3. Temperature of CPU increases with every instruction executed (and CPU is cooled by fan)

- For every listed side-channel, argue within the group (Google if necessary):
  - Propose an attack(s) based on the particular side-channel
  - What is the cost of required equipment?
  - What are possible options to mitigate the attack?
- Order given side-channels by
  - Seriousness with respect to security impact
  - Difficulty to systematically mitigate the side-channel leakage

CONCLUSIONS

Morale

1. Preventing implementation attacks is extra difficult
   – Naïve code is often vulnerable
     - Not aware of existing problems/attacks
   – Optimized code is often vulnerable
     - Time/power/acoustic… dependency on secret data
     - Dangerous optimizations (Infineon primes)
2. Use well-known libraries instead of own code
   – And follow security advisories and patch quickly
3. Security / mitigations are complex issues
   – Underlying hardware can leak information as well
   – Try to prevent large number of queries

Mandatory reading

- G. Goodwill, Defending against side-channel attacks
  - http://www.embedded.com/print/4408435
  - http://www.embedded.com/print/4409695
- Focus on:
  - What side channels are inspected?
  - What step in executed operation is misused for attack?
  - What are proposed defenses?

Conclusions

- Trusted element is secure anchor in a system
  - Understand why it is trusted and for whom
- Trusted element can be attacked
  - Non-invasive, semi-invasive, invasive methods
- Side-channel attacks are very powerful techniques
  - Attacks against particular implementation of algorithm
  - Attack possible even when algorithm is secure (e.g., AES)
- Use well-know libraries instead own implementation