Timing attacks

Daniel J. Bernstein, Tanja Lange

University of Illinois at Chicago,
Ruhr University Bochum;
Eindhoven University of Technology

ZDNet | SCANDINAVIA | AFRICA | UK | ITALY | SPAIN | MORE | NEWSLETTERS | ALL WRITERS

Minerva attack can recover private keys from smart cards, cryptographic libraries

Older Athena IDProtect smart cards are impacted, along with the WolfSSL, MatrixSSL, Crypto++, Oracle SunEC, and Libgcrypt crypto libraries.

By Catalin Cimpanu for Zero Day | October 3, 2019 -- 12:54 GMT (13:54 BST) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Google Chrome impacted by new Magellan 2.0 vulnerabilities

Security
Russia successfully disconnected from the internet

ZDNet article

ZDNet AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: How the CIO fought their way back from the edge of extinction

TPM-FAIL vulnerabilities impact TPM chips in desktops, laptops, servers

TPM-FAIL lets attackers steal private keys from TPMs. Attacks take from minutes to a few hours.

By Catalin Cimpanu for Zero Day | November 13, 2019 -- 04:23 GMT (04:23 GMT) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Google Chrome impacted by new Magellan 2.0 vulnerabilities

Security
Russia successfully disconnected from the internet

ZDNet article

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE **SECURITY** DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH
BOOTNOTES LECTURES

Security

Don't trust the Trusted Platform Module – it may leak your VPN server's private key (depending on your configuration)

You know what they say: Timing is... everything

By Thomas Claburn in San Francisco 12 Nov 2019 at 19:43

19 SHARE ▼

MOST READ


What's that? Encryption's OK now? UK politicos Brexit from Whatsapp to Signal


UK's Virgin Media celebrates the end of 2019 with a good, old fashioned TITSUP*


Starliner: Boeing, Boeing... it's back! Borked capsule makes a successful return to Earth

Patch now: Published Citrix applications leave networks of 'potentially 80,000' firms at risk from

Register article

golem.de
IT-NEWS FÜR PROFIS

HOME TICKER VIDEOS VORGELESEN FORUM | ANMELD Suchen

Golem.de jetzt werbefrei lesen TOP-THEMEN:

IT-KARRIERE: STELLENMARKT SEMINARE IT-KÖPFE GEHALTSCHECK | SERVICES: PREISVERGLEICH

mehr...

ELLIPTISCHE KURVEN

Minerva-Angriff zielt auf zertifizierte Krypto-Chips

Forscher konnten zeigen, wie sie mit einem Timing-Angriff die privaten Schlüssel von Signaturen mit elliptischen Kurven auslesen konnten. Verwundbar sind Chips, deren Sicherheit eigentlich zertifiziert wurde.

4. Oktober 2019, 13:41 Uhr, Hanno Böck

s Hollar, Wikimedia Commons)

Golem article

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ...

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ...

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ..., `IKK` takes slightly longer to fail.
Try `IKA`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ..., `IKK` takes slightly longer to fail.
Try `IKA`, `IKB`,

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ..., `IKK` takes slightly longer to fail.
Try `IKA`, `IKB`, `IKC`, ...

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ..., `IKK` takes slightly longer to fail.
Try `IKA`, `IKB`, `IKC`, ..., `IKV` takes slightly longer to fail.

⋮

Timing attacks are not a new phenomenon

Password recovery if server compares letter by letter:

Try `AAA`, `BBB`, `CCC`, ..., `III` takes slightly longer to fail.
Try `IAA`, `IBB`, `ICC`, ..., `IKK` takes slightly longer to fail.
Try `IKA`, `IKB`, `IKC`, ..., `IKV` takes slightly longer to fail.

⋮

Password is `IKVROCKS`.

1974: Exploit developed by Alan Bell for TENEX operating system.

Exponentiation with secret exponent (RSA, DH)

Compute c^d given c and d.

```
n = 1000001
d = 12473
c = 41241
l = d.nbits()
D = d.bits()
m = c
for i in range(l-2,-1,-1):
  m = m^2 % n
  if D[i] == 1:
    m = m * c % n
print(m)
```

Exponentiation with secret exponent (RSA, DH)

Compute c^d given c and d.

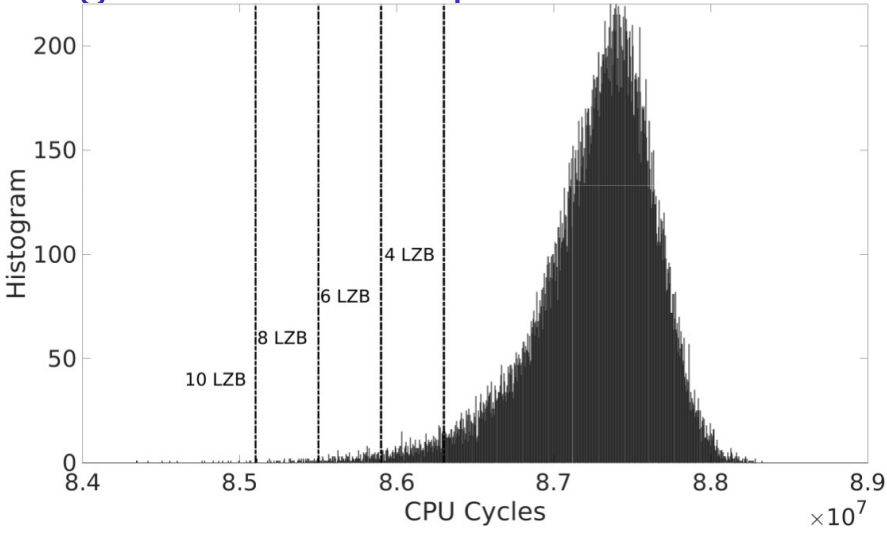
```
n = 1000001
d = 12473
c = 41241
l = d.nbits()
D = d.bits()
m = c
for i in range(l-2,-1,-1): # loop length depends on d
  m = m^2 % n
  if D[i] == 1:
    m = m * c % n
print(m)
```

Exponentiation with secret exponent (RSA, DH)

Compute c^d given c and d.

```
n = 1000001
d = 12473
c = 41241
l = d.nbits()
D = d.bits()
m = c
for i in range(l-2,-1,-1): # loop length depends on d
  m = m^2 % n
  if D[i] == 1: # branch depends on d
    m = m * c % n
print(m)
```

Timings of scalar multiplication on NIST P-256



(Picture from TPM-Fail)

Other exponentiation methods

- The timing variation depends strongly on the length of the scalar/exponent.
- Very sparse or very dense scalars will be miscategorized.
- Faster methods reduce the number of multiplications by using windows: $14019 =$

Other exponentiation methods

- The timing variation depends strongly on the length of the scalar/exponent.
- Very sparse or very dense scalars will be miscategorized.
- Faster methods reduce the number of multiplications by using windows: $14019 = \texttt{0x36C3} = \texttt{0011 0110 1100 0011}$

Other exponentiation methods

- The timing variation depends strongly on the length of the scalar/exponent.
- Very sparse or very dense scalars will be miscategorized.
- Faster methods reduce the number of multiplications by using windows: $14019 = \texttt{0x36C3} = \underbrace{0011}_{0\ 3}\ \underbrace{0110}_{1\ 2}\ \underbrace{1100}_{3\ 0}\ \underbrace{0011}_{0\ 3}$

Other exponentiation methods

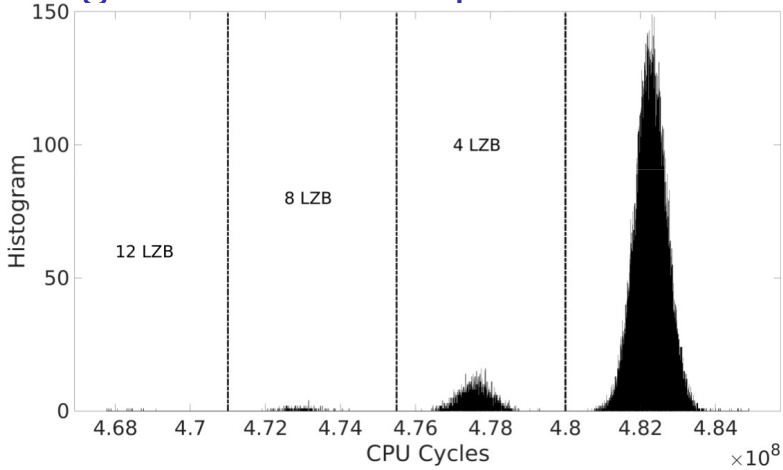
- The timing variation depends strongly on the length of the scalar/exponent.
- Very sparse or very dense scalars will be miscategorized.
- Faster methods reduce the number of multiplications by using windows: $14019 = \texttt{0x36C3} = \underbrace{0011}_{0\ 3}\ \underbrace{0110}_{1\ 2}\ \underbrace{1100}_{3\ 0}\ \underbrace{0011}_{0\ 3}$

  Precompute c, c^2, and c^3.

$$c^{14019} = \left(\left(\left(\left(\left(\left(c^3\right)^4 \cdot c\right)^4 \cdot c^2\right)^4 \cdot c^3\right)^4\right)^4\right)^4 \cdot c^3.$$

  Same number of squarings, 4 instead of 7 multiplications.

Timings of scalar multiplication on NIST P-256



Larger windows reduce the variability through branching but accentuate the length.

(Picture from TPM-Fail)

How much can a few bits do?

- A bit for RSA, DH, etc.

How much can a few bits do?

- A bit for RSA, DH, etc. More for RSA with CRT decryption.

How much can a few bits do?

- A bit for RSA, DH, etc. More for RSA with CRT decryption.
- A lot for DSA and ECDSA signatures:
  - TPM–Fail: TPM meets Timing and Lattice Attacks
    Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, Nadia Heninger
    https://tpm.fail/
  - Minerva attack
    Jan Jancar, Petr Svenda, Vladimir Sedlacek
    https://minerva.crocs.fi.muni.cz/

  With just a small bias in the nonces (one-time scalars) the secret signing key leaks.

How much can a few bits do?

- A bit for RSA, DH, etc. More for RSA with CRT decryption.
- A lot for DSA and ECDSA signatures:
  - TPM–Fail: TPM meets Timing and Lattice Attacks
    Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, Nadia Heninger
    https://tpm.fail/
  - Minerva attack
    Jan Jancar, Petr Svenda, Vladimir Sedlacek
    https://minerva.crocs.fi.muni.cz/

  With just a small bias in the nonces (one-time scalars) the secret signing key leaks.
- Lots of libraries, smart cards, and TPMs affected.

How much can a few bits do?

- A bit for RSA, DH, etc. More for RSA with CRT decryption.
- A lot for DSA and ECDSA signatures:
  - TPM–Fail: TPM meets Timing and Lattice Attacks
    Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, Nadia Heninger
    https://tpm.fail/
  - Minerva attack
    Jan Jancar, Petr Svenda, Vladimir Sedlacek
    https://minerva.crocs.fi.muni.cz/

  With just a small bias in the nonces (one-time scalars) the secret signing key leaks.
- Lots of libraries, smart cards, and TPMs affected.
- Even worse: hyperthreading attacks, cache-timing attacks, etc. give more fine-grained timing information $\Rightarrow$ more exploits.

Constant-time exponentiation

```
n = 1000001
d = 12473
c = 41241
l = n.nbits()
D = d.digits(2,padto = l)
m = 1 # so initial squarings don't matter
for i in range(l-1,-1,-1): # fixed-length loop
  m = m^2 % n
  h = m * c % n
  m = (1 - D[i]) * m + D[i] * h # selection by arithmetic
print(m)
```

This costs 1 multiplication per bit, so as slow as worst case.

Interplay with elliptic-curve formulas

- We can translate this to scalar multiplication on elliptic curves: Initialize with the neutral element, for every bit compute a doubling and an addition.
- Formulas for addition on Weierstrass curves have exceptions for adding ∞, so initialization at ∞ does not work.
- Edwards curves have a complete addition law, **easy** to double or add the neutral element $(0, 1)$.
- The Montgomery ladder has a similar data flow, but the costs per bit of the scalar are **less** than one addition plus one doubling for Montgomery curves.

For more see https://ecchacks.cr.yp.to.