Every Threat Model is Wrong

Daniel Gruss

Graz University of Technology

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

GLOSSARY

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

threat modeling

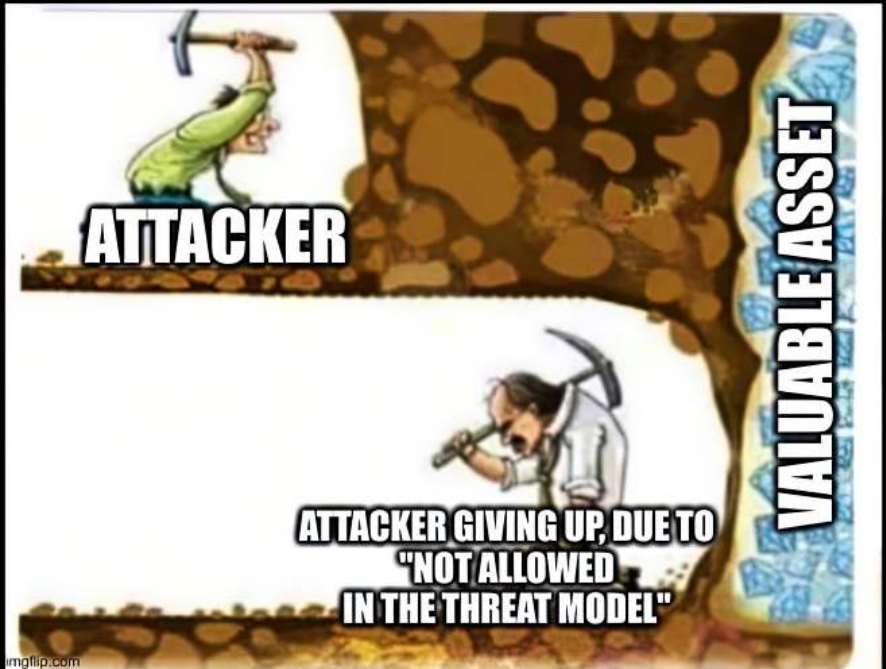
Definitions:

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.

Sources:

NIST SP 800-53 Rev. 5

Search


ATTACKER
ATTACKER GIVING UP, DUE TO
"NOT ALLOWED
IN THE THREAT MODEL"
VALUABLE ASSET
imgflip.com

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

GLOSSARY

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

threat modeling

Definitions:

A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment.

Sources:

NIST SP 800-53 Rev. 5

Search

What my friends think I do

What my parents think I do

What professionals think I do

What the NSA thinks I do

What I think I do

What I actually do

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

Page Not Found

Trying to find a specific publication? Visit our publications homepage or see lists of Draft Publications, FIPS, SP 800s, and all final NIST cybersecurity and privacy publications.

The page you were looking for cannot be found. If this was unexpected behavior, please send an email to csrc-inquiry@nist.gov. Make sure to include a detailed description of the actions you took and the page ultimately referred you here.

https://csrc.nist.gov/glossary/term/term_that_does_not_exist

An official website of the United States government Here's how you know

NIST

Sear

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NI

Projects

Publications +

Topics +

News & Updates

Events

Page Not Found

Trying to find a specific publication? Visit our publications hor
Publications, FIPS, SP 800s, and all final NIST cybersecurity ar

The page you were looking for cannot be found. If this was unex
to csrc-inquiry@nist.gov. Make sure to include a detailed descr
page ultimately referred you here.

security

Models

Models

Models

Models

- Model could be more generic than reality

Models

- Model could be more generic than reality
- Good as long as it's more pessimistic than reality

Models

- Model could be more generic than reality
- Good as long as it's more pessimistic than reality

Models

- Model could be more generic than reality
- Good as long as it's more pessimistic than reality, right?

Models

- Model could be more generic than reality
- Good as long as it's more pessimistic than reality, right?
- Only true as long as there is no adversary

Models

- Model could be more generic than reality
- Good as long as it's more pessimistic than reality, right?
- Only true as long as there is no adversary
- Adversary: just step outside the threat model and attack the system differently

Example

Example

Example

Example

- A bug in some user software was not really a security problem but (possibly) a reliability problem

Example

- A bug in some user software was not really a security problem but (possibly) a reliability problem
- local exploitation $\rightarrow$ how does the attacker even get there

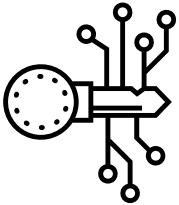
Example

- A bug in some user software was not really a security problem but (possibly) a reliability problem
- local exploitation $\rightarrow$ how does the attacker even get there
- was less dangerous before the Internet

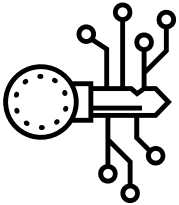
With the Internet, there's always an adversary.

Another Example

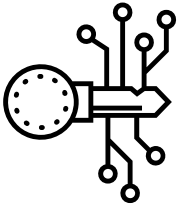
Another Example



Another Example

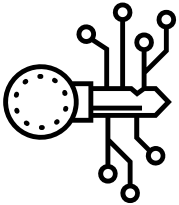


Another Example



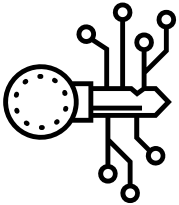
- A cryptographic implementation

Another Example



- A cryptographic implementation
- Threat model: all kinds of assumptions on security of cipher, correct implementation, mathematical foundations, etc.

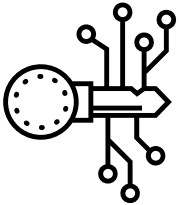
Another Example



- A cryptographic implementation
- Threat model: all kinds of assumptions on security of cipher, correct implementation, mathematical foundations, etc.

$\rightarrow$ one step outside the threat model: side channels

Another Example



- A cryptographic implementation
- Threat model: all kinds of assumptions on security of cipher, correct implementation, mathematical foundations, etc.

→ one step outside the threat model: side channels

- cryptographers generally consider these for the design of the cipher but ...

Security Policy

Threat Model

Certain threats are currently considered outside of the scope of the OpenSSL threat model. Accordingly, we do not consider OpenSSL secure against the following classes of attacks:

- same physical system side channel
- CPU/hardware flaws
- physical fault injection
- physical observation side channels (e.g. power consumption, EM emissions, etc)

Side Channels

Timing Side Channels

Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Paul C. Kocher

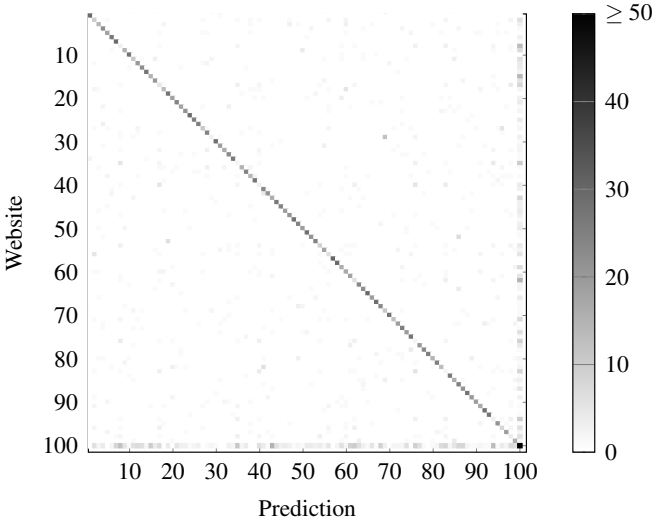
Cryptography Research, Inc.
~~607 Market Street, 5th Floor, San Francisco, CA 94105, USA.~~
~~E-mail: paul@cryptography.com.~~

Abstract. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-

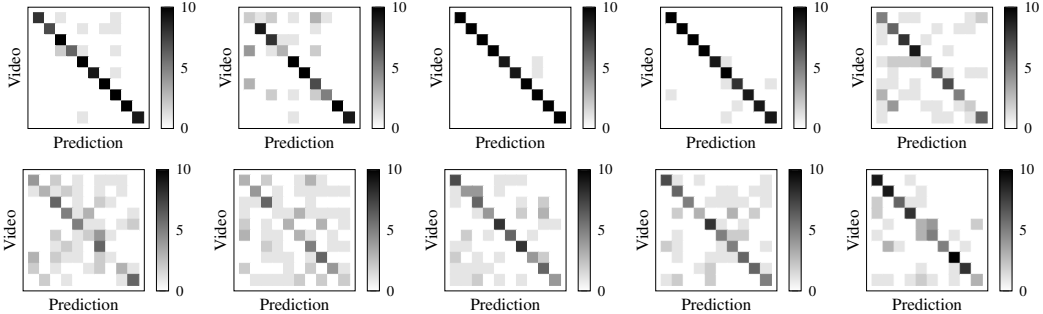

amazon.com
Prime+Probe
ROWHAMMERJS
ANOTHER FLIP IN THE ROW
FANTASTIC
TIMERS
AND WHERE
TO FIND THEM
HIGH-RESOLUTION MICROARCHITECTU
ATTACKS IN JAVASCRIPT
ALQ
JavaScript
zero
ÆPIC
LEAK
REAL
JavaScript
AND ZERO
SIDE-CHANNEL
ATTACKS

that can perform operations such as
multiplication and memory operations in parallel.

SnailLoad: Top-100 Open-World Website Fingerprinting



SnailLoad: Video Fingerprinting



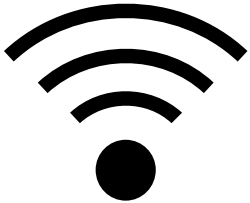
But what does that mean?

But what does that mean?

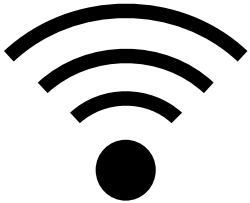
$\rightarrow$ **Demo!**

Is it part of our Threat Model?

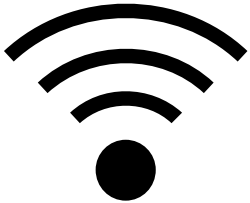
Is it part of our Threat Model?



Is it part of our Threat Model?

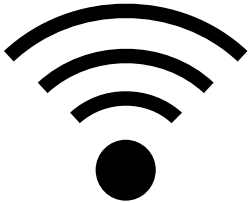


Is it part of our Threat Model?



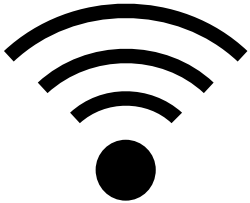
- Any connection can get traces of your activity $\rightarrow$ are all your connections trustworthy?

Is it part of our Threat Model?



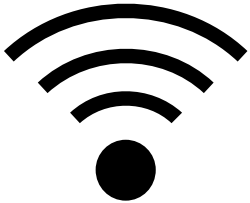
- Any connection can get traces of your activity → are all your connections trustworthy?
- Traces can leak websites and videos watched

Is it part of our Threat Model?



- Any connection can get traces of your activity → are all your connections trustworthy?
- Traces can leak websites and videos watched
- Not trivial to fix

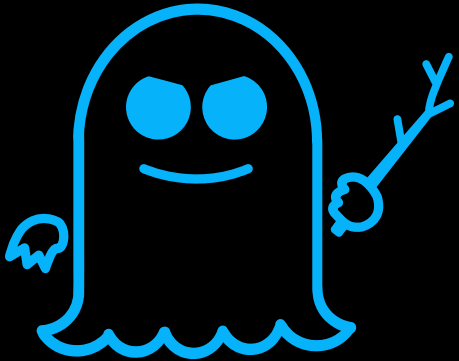
Is it part of our Threat Model?



- Any connection can get traces of your activity → are all your connections trustworthy?
- Traces can leak websites and videos watched
- Not trivial to fix

Try it out: `https://snailload.com`

MELTDOWN



SPECTRE

Fault Attacks

Fault Attacks

Fault Attacks

Fault Attacks

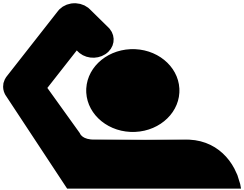
- Rowhammer, Plundervolt, ...

Fault Attacks

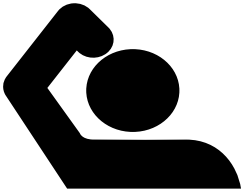
- Rowhammer, Plundervolt, ...
- commonly not part of threat models

Do Threat Models just reflect knowledge?

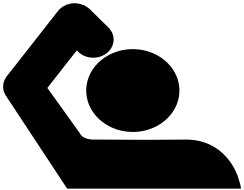
Do Threat Models just reflect knowledge?



Do Threat Models just reflect knowledge?

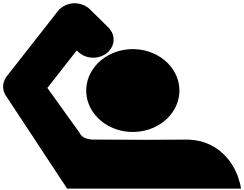


Do Threat Models just reflect knowledge?



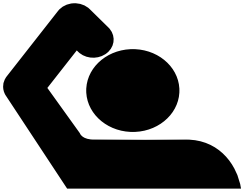
- Threat models now often adjusted for side channels, fault attacks, transient execution

Do Threat Models just reflect knowledge?



- Threat models now often adjusted for side channels, fault attacks, transient execution
- But not always! $\rightarrow$ it's not just a reflection of knowledge

Do Threat Models just reflect knowledge?



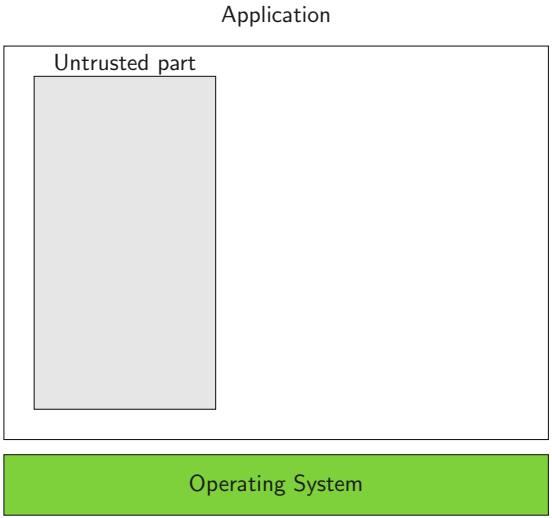
- Threat models now often adjusted for side channels, fault attacks, transient execution
- But not always! $\rightarrow$ it's not just a reflection of knowledge

$\rightarrow$ Often, we want to ignore the problem

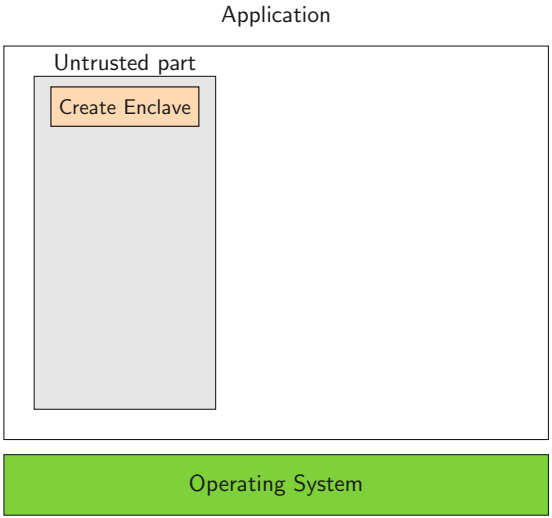
Ambitious Threat Models

Some threat models are so ambitious $\rightarrow$ difficult/impossible to keep

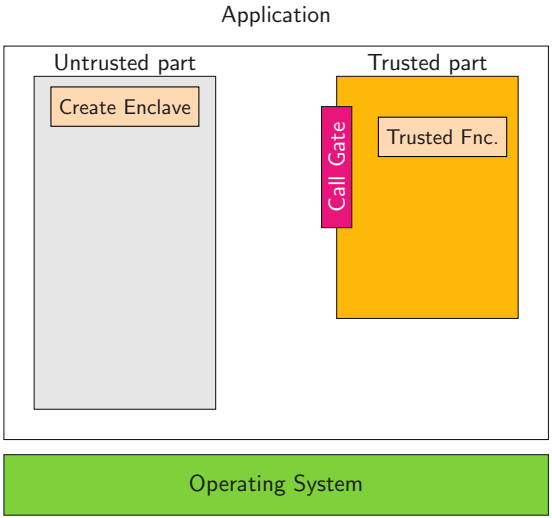
SGX



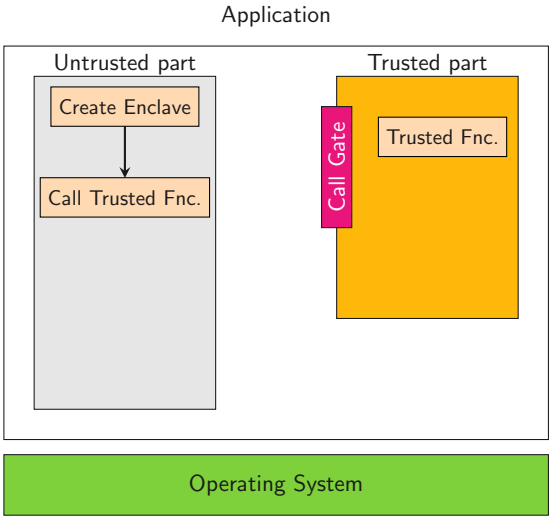
SGX


Application
Untrusted part
Create Enclave
Operating System

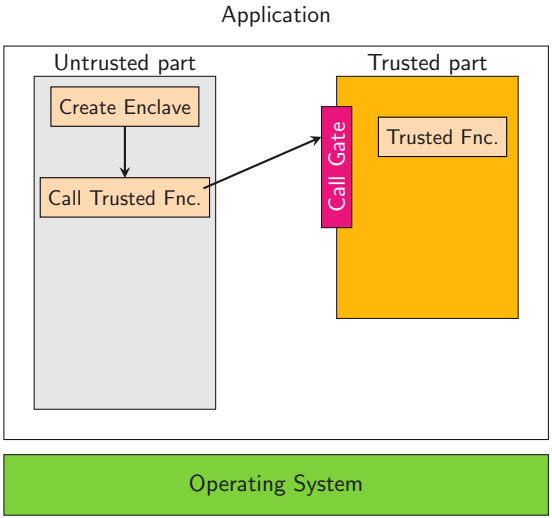
SGX


Application
Untrusted part
Create Enclave
Trusted part
Call Gate
Trusted Fnc.
Operating System

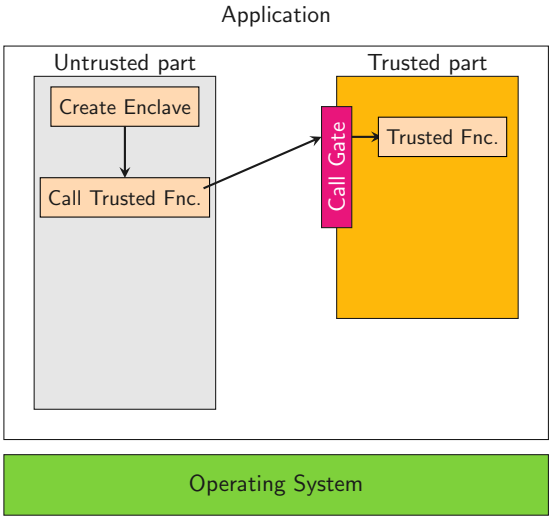
SGX


Application
Untrusted part
Create Enclave
Call Trusted Fnc.
Trusted part
Call Gate
Trusted Fnc.
Operating System

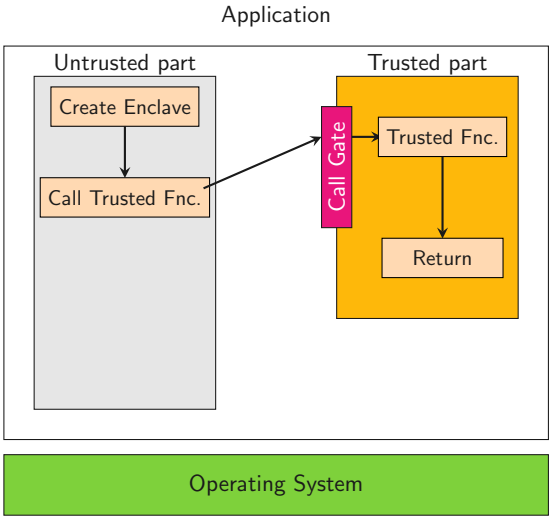
SGX


Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
Call Gate
Trusted Fnc.
Operating System

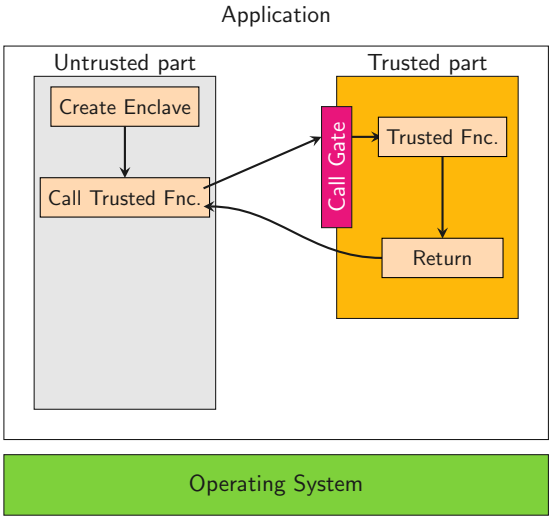
SGX


Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
Call Gate
Trusted Fnc.
Operating System

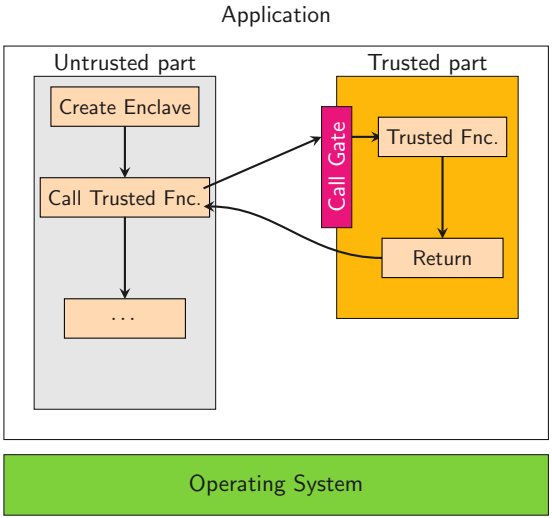
SGX


Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
Call Gate
Trusted Fnc.
Return
Operating System

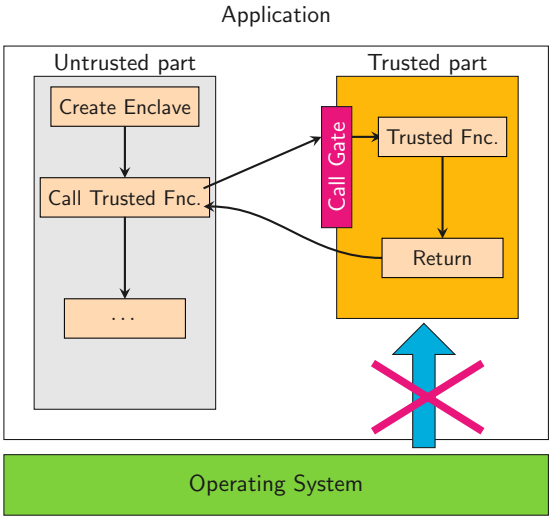
SGX


Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
Call Gate
Trusted Fnc.
Return
Operating System

SGX

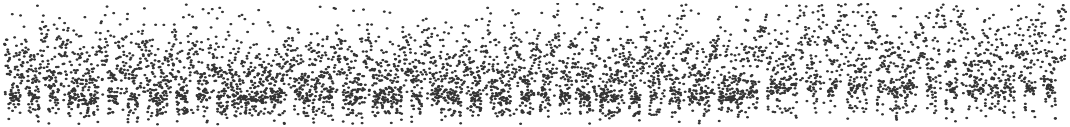

Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
...
Call Gate
Trusted Fnc.
Return
Operating System

SGX


Application
Untrusted part
Trusted part
Create Enclave
Call Trusted Fnc.
...
Call Gate
Trusted Fnc.
Return
Operating System

Measured Trace

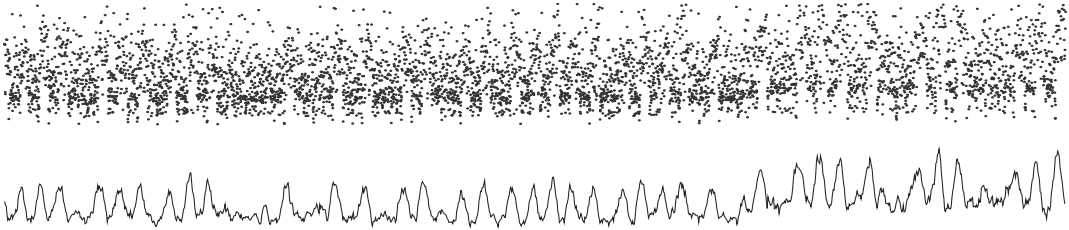
Raw Prime+Probe trace...



Malware Guard Extension: Using SGX to Conceal Cache Attacks.
Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, Stefan Mangard. DIMVA'17

Measured Trace

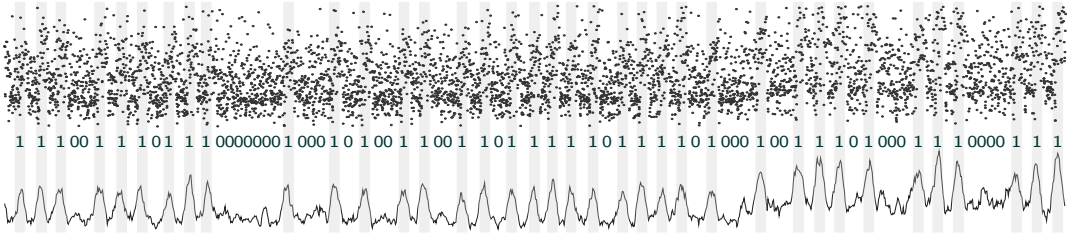
...processed with a simple moving average...



Malware Guard Extension: Using SGX to Conceal Cache Attacks.
Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, Stefan Mangard. DIMVA'17

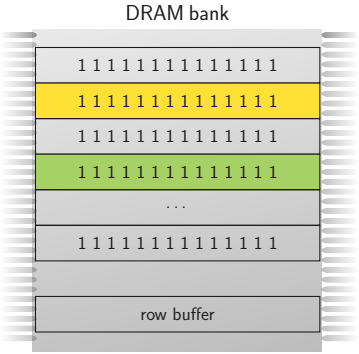
Measured Trace

...allows to clearly see the bits of the exponent



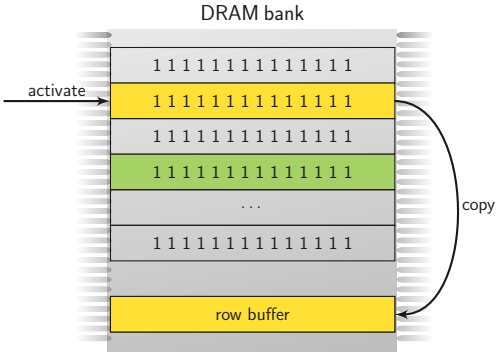
Malware Guard Extension: Using SGX to Conceal Cache Attacks.
Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, Stefan Mangard. DIMVA'17

Rowhammer



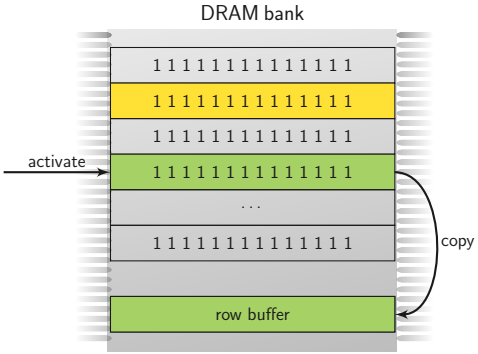
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



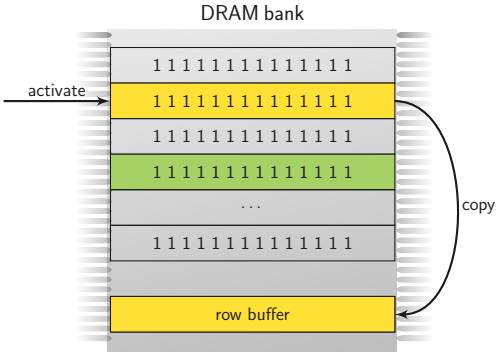
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



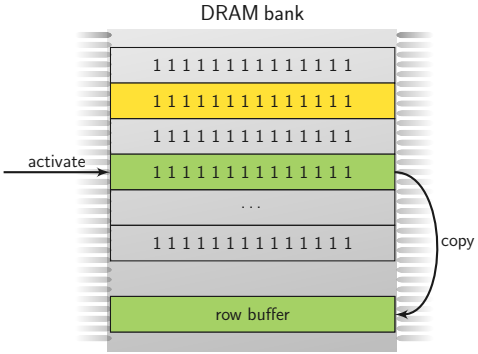
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



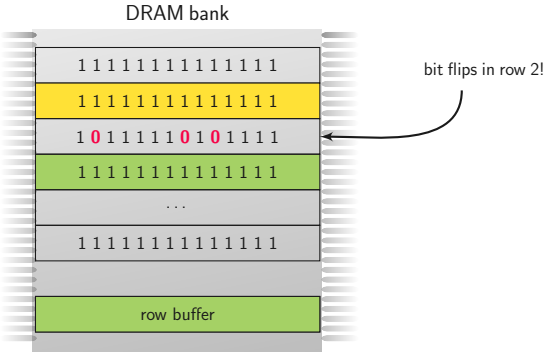
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



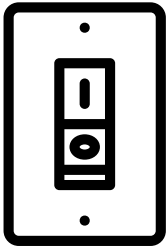
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



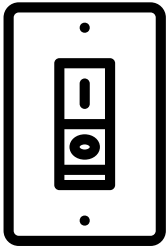
- Cells leak → repetitive refresh necessary
- Maximum interval between refreshes to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Bit Flips in SGX EPC Memory



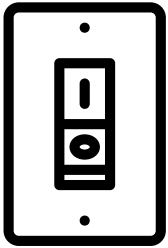
- What happens if a bit flips in the SGX EPC Memory?

Bit Flips in SGX EPC Memory



- What happens if a bit flips in the SGX EPC Memory?
- Integrity check will fail!

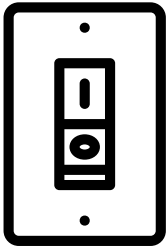
Bit Flips in SGX EPC Memory



- What happens if a bit flips in the SGX EPC Memory?
- Integrity check will fail!

→ Locks up the memory controller

Bit Flips in SGX EPC Memory



- What happens if a bit flips in the SGX EPC Memory?
- Integrity check will fail!

→ Locks up the memory controller

→ Entire System Denial-of-Service!

- **SGX Bomb** paper

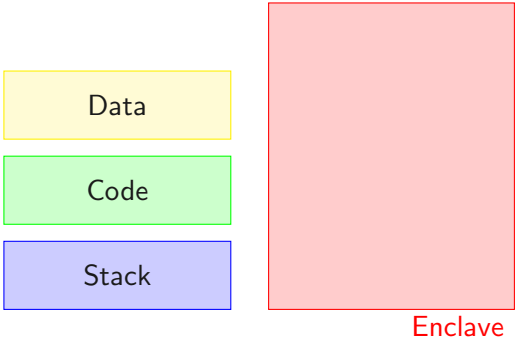

HIDE MY CODE
IN A TEE


HIDE A SIDE-CHANNEL
ATTACK IN A TEE

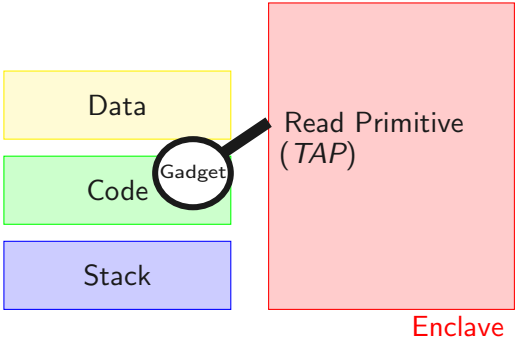

HIDE ROWHAMMER
DOS/PRIVESC IN A TEE


HIDE A ZERO
DAY IN A TEE
imgflip.com

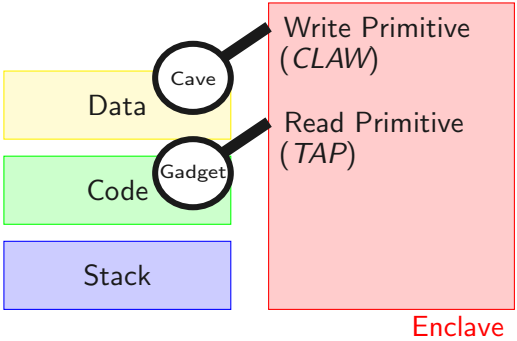
Hiding a Zero Day?



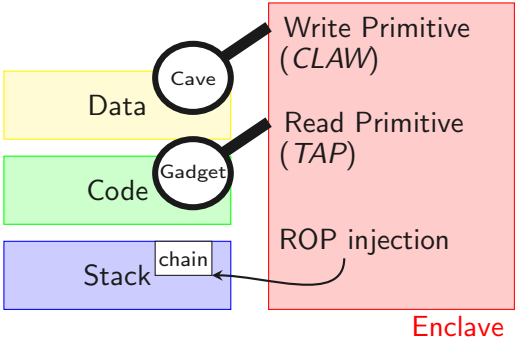
Hiding a Zero Day?



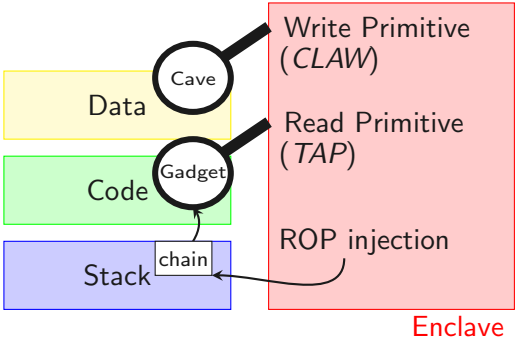
Hiding a Zero Day?



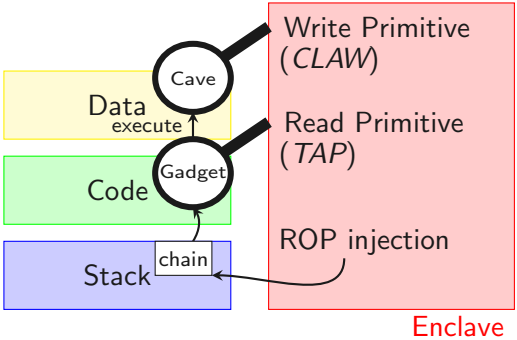
Hiding a Zero Day?



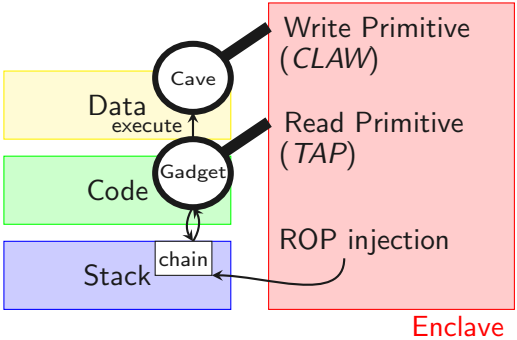
Hiding a Zero Day?



Hiding a Zero Day?

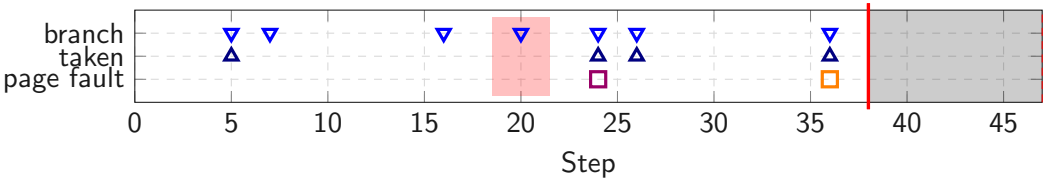


Hiding a Zero Day?



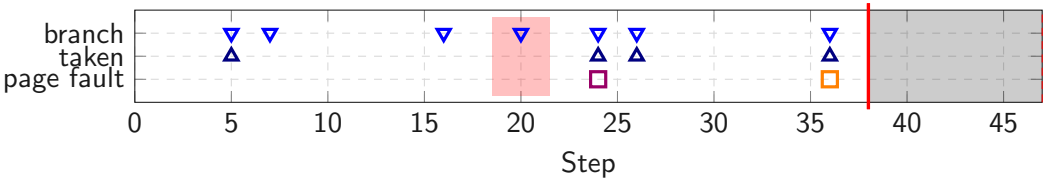
What about more recent TEEs?

Breaking Mbed TLS Square + Multiply

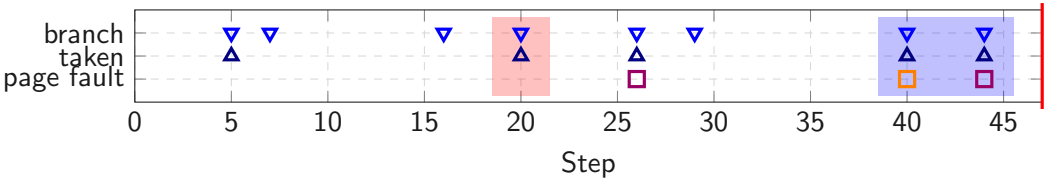


$\texttt{ei} = 0$

Breaking Mbed TLS Square + Multiply



$\texttt{ei} = 0$



$\texttt{ei} = 1$

Intel TDX / AMD SEV-SNP idea:

“Take any VM and run it as a CVM in our TEE”

Recovering TOTPs (memcmp-style)

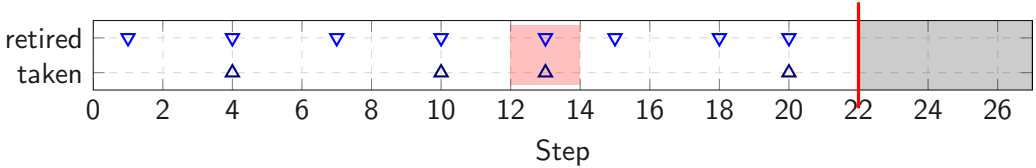
```
COTPRESULT totp_compare(OTPData* data, const char* key,
    int64_t offset, uint64_t for_time)
{
  char time_str[data->digits+1];
  memset(time_str, 0, data->digits+1);
  if (totp_at(data, for_time, offset, time_str) == 0)
    return OTP_ERROR;
  for (size_t i=0; i<data->digits; i++) {
    if (key[i] != time_str[i])
      return OTP_ERROR;
  }
  return OTP_OK;
}
```

Recovering TOTPs (memcmp-style)

```
COTPRESULT totp_compare(OTPData* data, const char* key,
    int64_t offset, uint64_t for_time)
{
  char time_str[data->digits+1];
  memset(time_str, 0, data->digits+1);
  if (totp_at(data, for_time, offset, time_str) == 0)
    return OTP_ERROR;
  for (size_t i=0; i<data->digits; i++) {
    if (key[i] != time_str[i])
      return OTP_ERROR;
  }
  return OTP_OK;
}
```

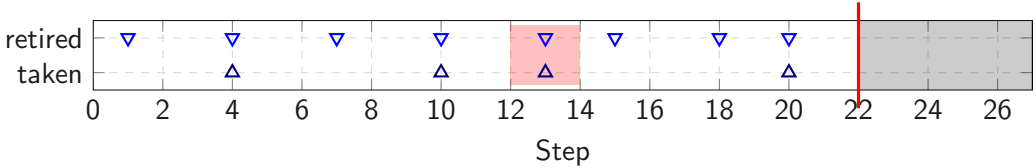
Guess the TOTP digit-by-digit with at most 60 attempts, instead of 1 000 000

Recovering TOTPs (memcmp-style)

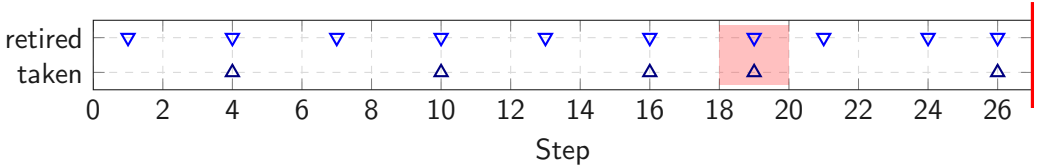


2 correct digits

Recovering TOTPs (memcmp-style)



2 correct digits



3 correct digits

Problems around CVM concept

Problems around CVM concept

Problems around CVM concept

Problems around CVM concept

- Vendor response: “make it constant time”

Problems around CVM concept

- Vendor response: "make it constant time"

→ General purpose code can't be made constant time → can still be attacked

Problems around CVM concept

- Vendor response: "make it constant time"

→ General purpose code can't be made constant time → can still be attacked

- Vendor response: "not part of our threat model"

Problems around CVM concept

- Vendor response: "make it constant time"

→ General purpose code can't be made constant time → can still be attacked

- Vendor response: "not part of our threat model"

→ but the attack works, what now!?

Problems around CVM concept

- Vendor response: "make it constant time"

→ General purpose code can't be made constant time → can still be attacked

- Vendor response: "not part of our threat model"

→ but the attack works, what now!?

- Vendor response: "does not create any new attack surface"

Problems around CVM concept

- Vendor response: "make it constant time"

→ General purpose code can't be made constant time → can still be attacked

- Vendor response: "not part of our threat model"

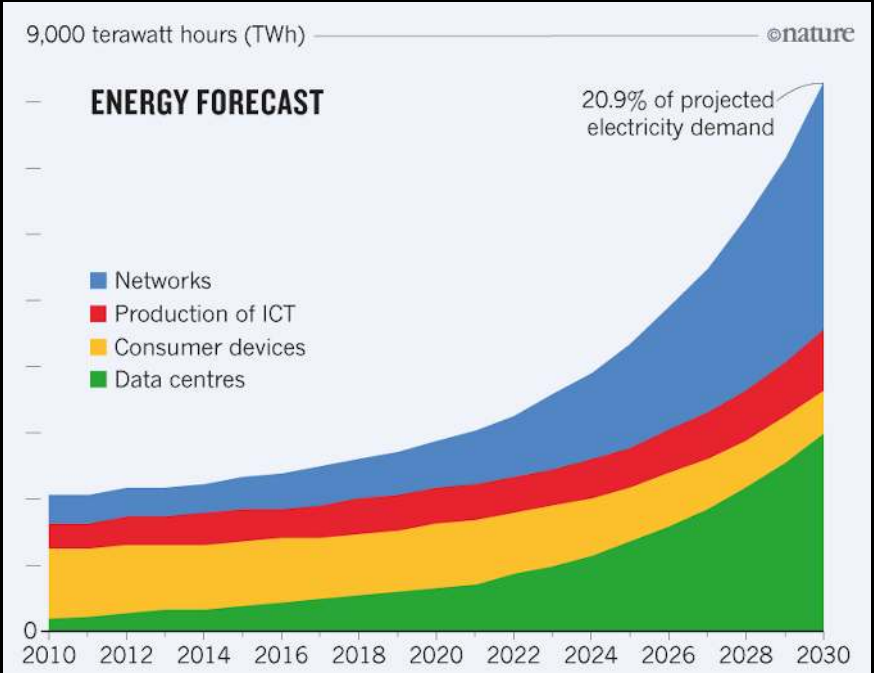
→ but the attack works, what now!?

- Vendor response: "does not create any new attack surface"

→ maybe true but the landscape changes

We cannot model all threats.

Threat: Security gets too expensive.

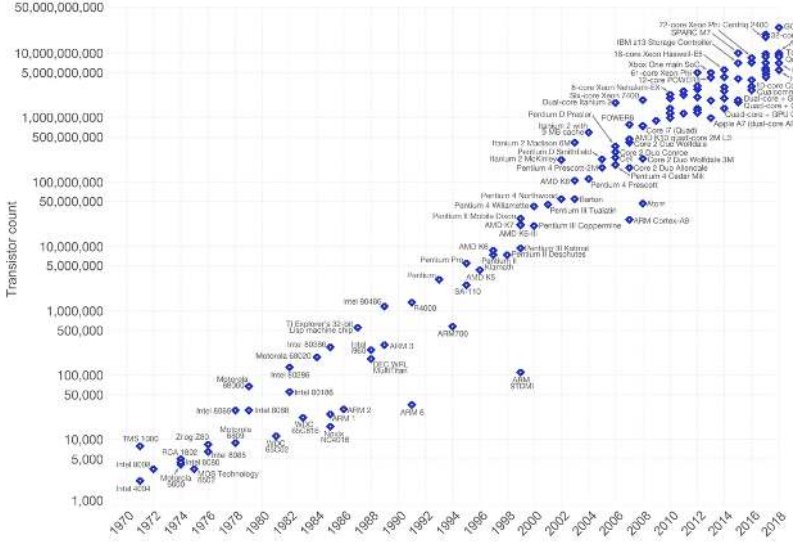

9,000 terawatt hours (TWh)
©nature
ENERGY FORECAST
20.9% of projected electricity demand
Networks
Production of ICT
Consumer devices
Data centres
0
2010
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030

0.09%

0.40%

Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

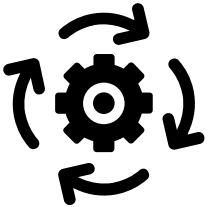
Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

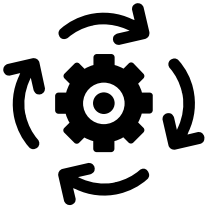
But security costs! And stuff like Rowhammer is dangerous!

Principled Cryptographic Security and Integrity



Make bit flips degrade performance **without** impacting security

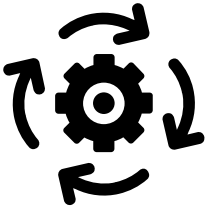
Principled Cryptographic Security and Integrity



Make bit flips degrade performance **without** impacting security

- Cryptographic MAC

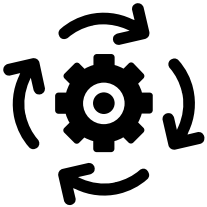
Principled Cryptographic Security and Integrity



Make bit flips degrade performance **without** impacting security

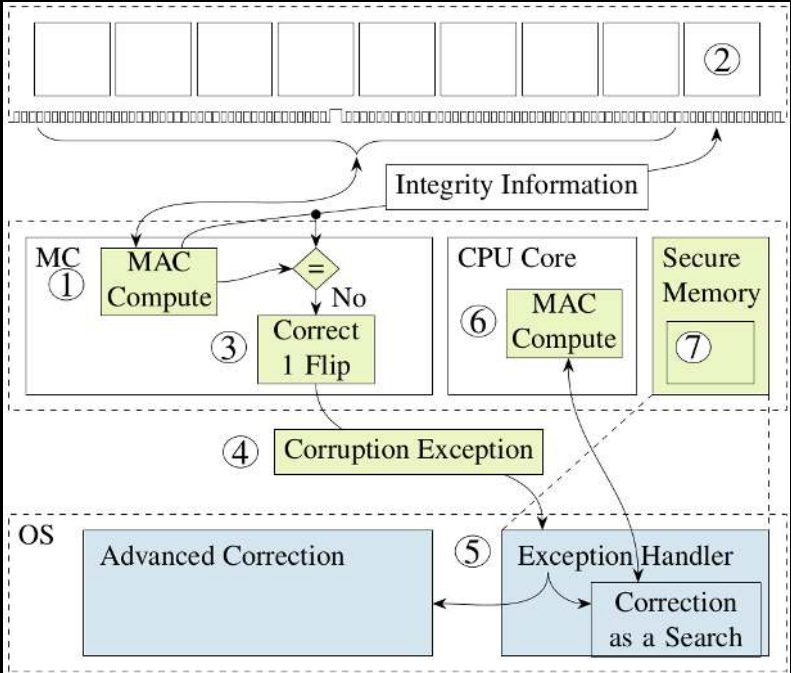
- Cryptographic MAC
- Detect **any** number of bit flips

Principled Cryptographic Security and Integrity

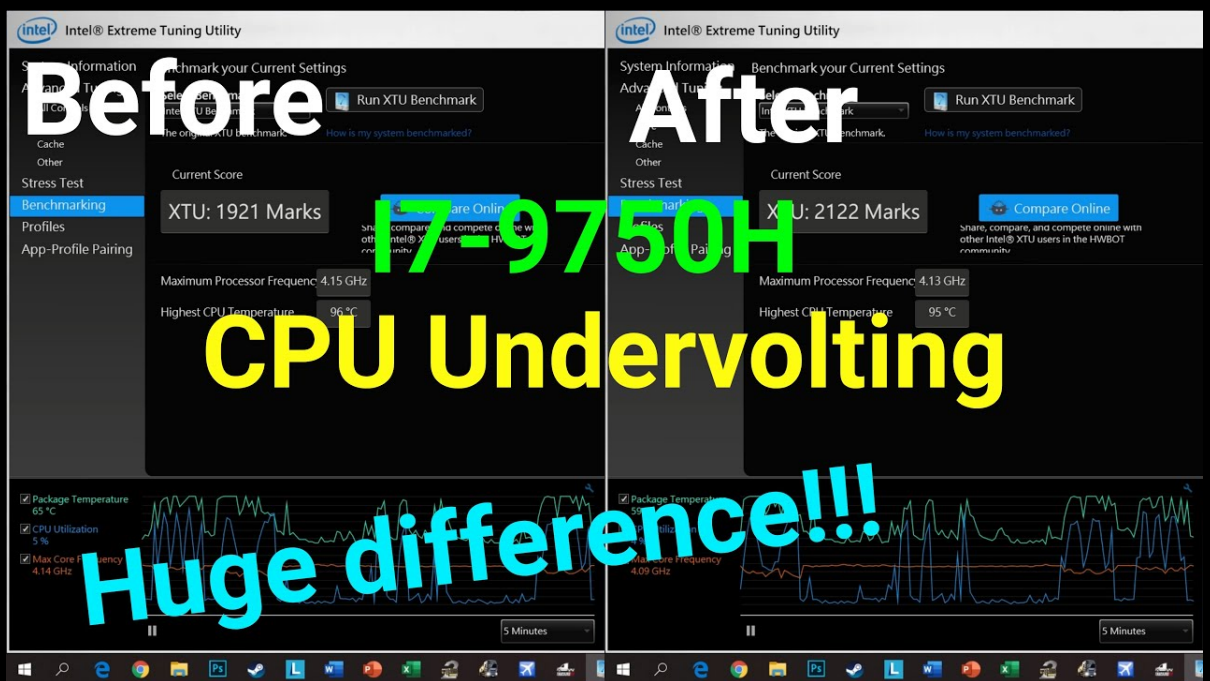


Make bit flips degrade performance **without** impacting security

- Cryptographic MAC
- Detect **any** number of bit flips
- Correction by **brute-force** search for correct data

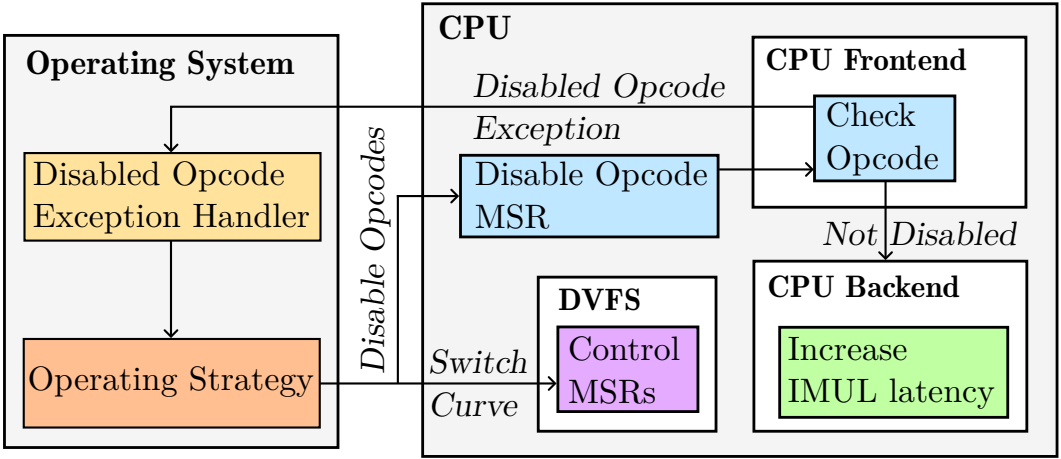

2
Integrity Information
MC
1
MAC
Compute
=
No
3
Correct
1 Flip
CPU Core
6
MAC
Compute
Secure
Memory
7
4
Corruption Exception
OS
Advanced Correction
5
Exception Handler
Correction
as a Search

Undervolting


Before
After
i7-9750H
CPU Undervolting
Huge difference!!!
Intel® Extreme Tuning Utility
Benchmark your Current Settings
Run XTU Benchmark
How is my system benchmarked?
Cache
Other
Stress Test
Benchmarking
Profiles
App-Profile Pairing
Current Score
XTU: 1921 Marks
Maximum Processor Frequenc 4.15 GHz
Highest CPU Temperature 96 °C
Package Temperature 65 °C
CPU Utilization 5 %
Max Core Frequency 4.14 GHz
5 Minutes
Intel® Extreme Tuning Utility
Benchmark your Current Settings
Run XTU Benchmark
How is my system benchmarked?
Cache
Other
Stress Test
Current Score
XTU: 2122 Marks
Compare Online
Share, compare, and compete online with other Intel® XTU users in the HWBOT community
Maximum Processor Frequenc 4.13 GHz
Highest CPU Temperature 95 °C
Max Core Frequency 4.09 GHz
5 Minutes

PLUNDER VOLT

SUIT - Secure Undervolting



Performance Improvement and Power Savings

CPU	V_{off}	Score	Power	Freq.	Energy Eff.
i5-1035G1	−70 mV	+6.0 %	−0.1 %	+8.5 %	+6.1 %
	−97 mV	+7.9 %	−0.5 %	+12 %	+8.4 %
i9-9900K	−70 mV	+2.2 %	−7.2 %	+2.6 %	+10 %
	−97 mV	+3.8 %	−16 %	+3.3 %	+23 %
7700X*	−70 mV	+1.4 %	−9.8 %	+1.8 %	+12 %
	−97 mV	+1.9 %	−15 %	+1.8 %	+20 %

Projects

Publications +

Topics +

News & Updates

Events

Glossary

About CSRC +

Page Not Found

Trying to find a specific publication? Visit our publications homepage or see lists of Draft Publications, FIPS, SP 800s, and all final NIST cybersecurity and privacy publications.

The page you were looking for cannot be found. If this was unexpected behavior, please send an email to csrc-inquiry@nist.gov. Make sure to include a detailed description of the actions you took and the page ultimately referred you here.

What is our collective vendor response?

Same in the real world as in security:

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza - "not part of our threat model"

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"? - "not part of our threat model"

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever - "just make things constant-time"-equivalent

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever - "just make it illegal to kill journalists"

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever
- Allied states curtailing democracy

What is our collective vendor response?

Same in the real world as in security:

- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever
- Allied states curtailing democracy - "we don't think this creates any new attack surface"-equivalent

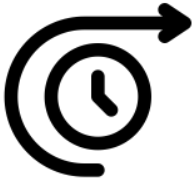
What is our collective vendor response?

Same in the real world as in security:

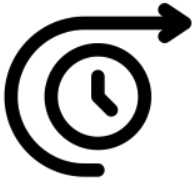
- USA "owning" Canada/Greenland/Gaza
- USA allying with Russia against Ukrainian "dictatorship"?
- 2024 deadliest year for journalists ever
- Allied states curtailing democracy- "we don't think anything changed"

A Path Forward!

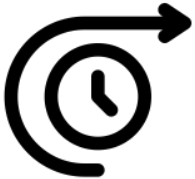
A Path Forward!



A Path Forward!

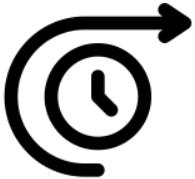


A Path Forward!



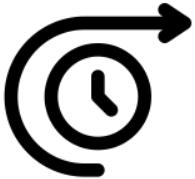
- Science: Models can never reach reality - getting arbitrarily close gets arbitrarily complex

A Path Forward!



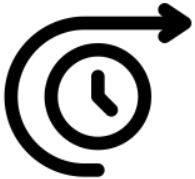
- Science: Models can never reach reality - getting arbitrarily close gets arbitrarily complex
- Split up (our view on) threat models:

A Path Forward!



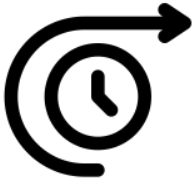
- Science: Models can never reach reality - getting arbitrarily close gets arbitrarily complex
- Split up (our view on) threat models:
  - What do we aim to defend against?

A Path Forward!



- Science: Models can never reach reality - getting arbitrarily close gets arbitrarily complex
- Split up (our view on) threat models:
  - What do we aim to defend against?
  - What are threats that we don't know how to handle?

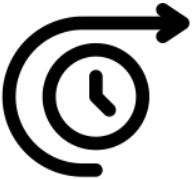
A Path Forward!



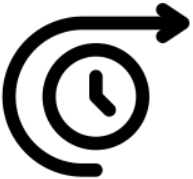
- Science: Models can never reach reality - getting arbitrarily close gets arbitrarily complex
- Split up (our view on) threat models:
  - What do we aim to defend against?
  - What are threats that we don't know how to handle?
- "Not in the threat model" is almost nonsensical

A Path Forward!

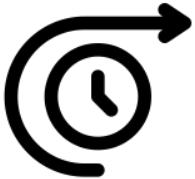
A Path Forward!



A Path Forward!

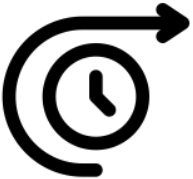


A Path Forward!



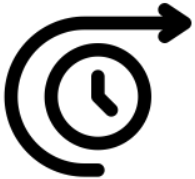
- Threat-model oriented research $\rightarrow$ what is **not** in the threat model? $\rightarrow$ focus on that

A Path Forward!



- Threat-model oriented research $\rightarrow$ what is **not** in the threat model? $\rightarrow$ focus on that
- Threat-model oriented thinking $\rightarrow$ what would be a problem, not what we can expect

A Path Forward!



- Threat-model oriented research → what is **not** in the threat model? → focus on that
- Threat-model oriented thinking → what would be a problem, not what we can expect
- What we can expect changes all the time!

Every Threat Model is Wrong

Daniel Gruss

Graz University of Technology