UNIVERSITÉ Concordia UNIVERSITY

NDSS 2019, San Diego, USA, Feb 24-27, 2019

TEE-aided Write Protection Against Privileged Data Tampering

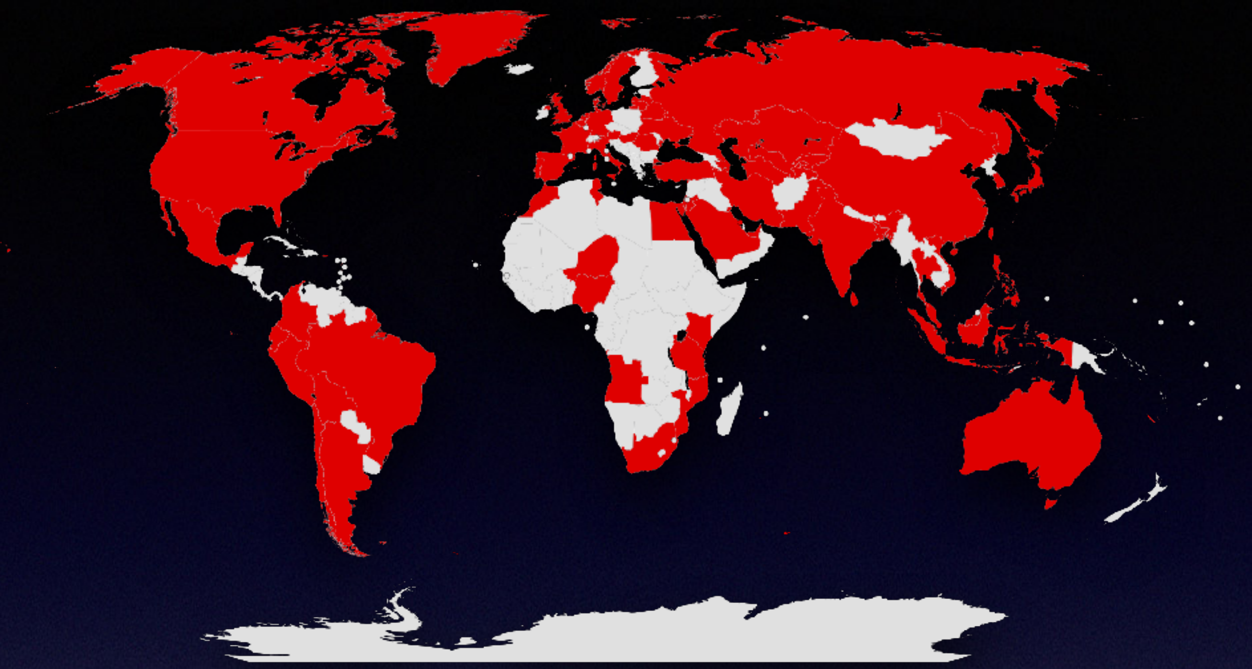
Lianying Zhao, University of Toronto
Mohammad Mannan, Concordia University, Canada

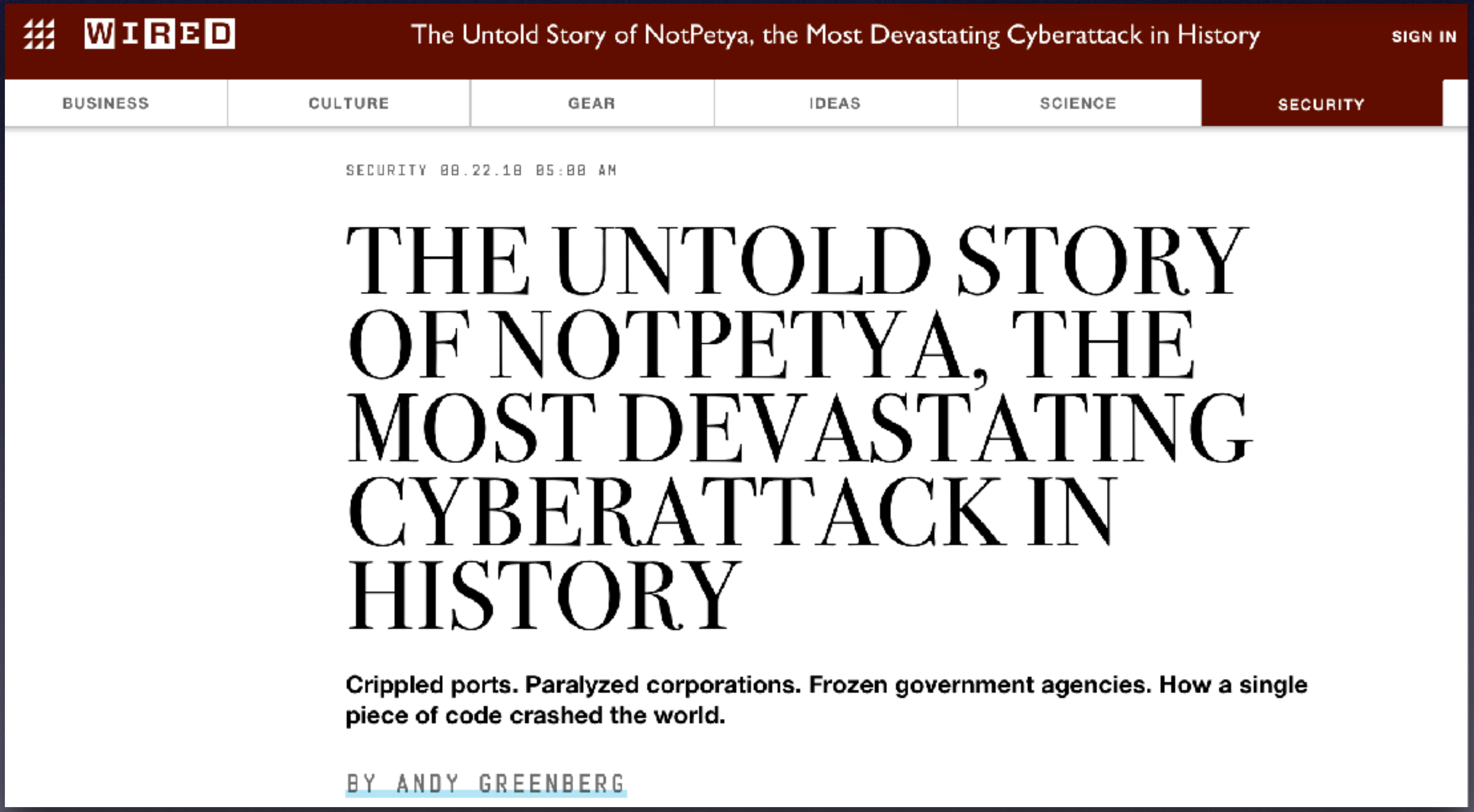
Ransomware

+

Data destruction malware

WannaCry: ~4-8 billion
NotPetya: ~10 billion USD





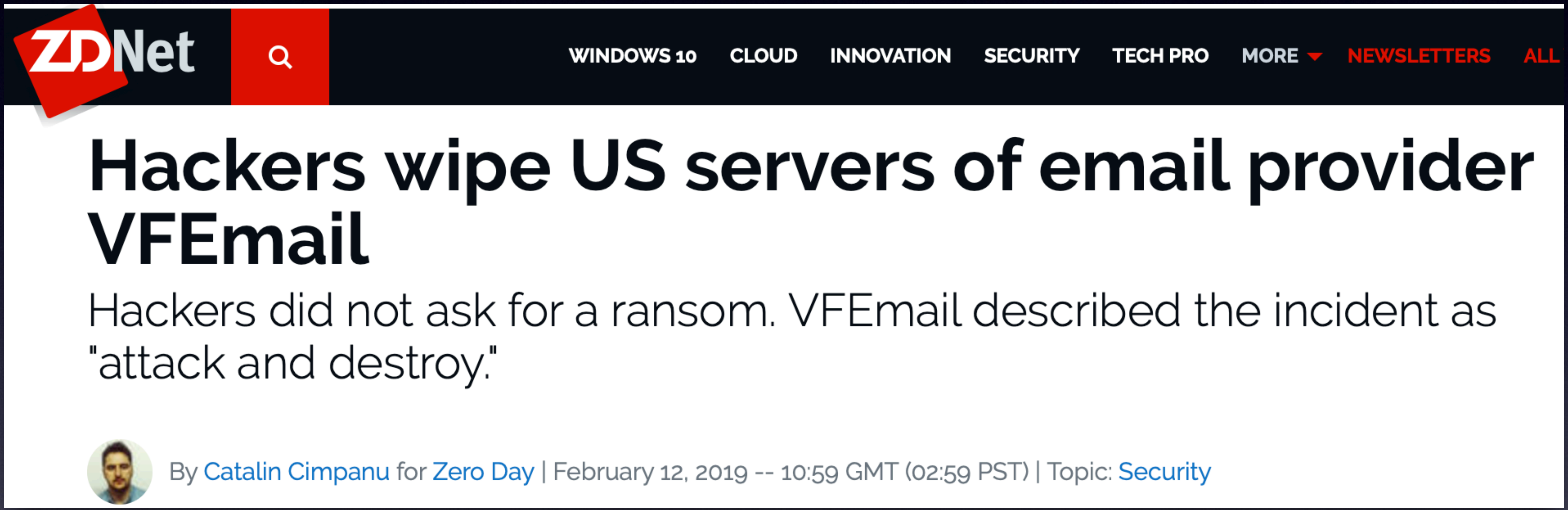
WIRED
The Untold Story of NotPetya, the Most Devastating Cyberattack in History
SIGN IN
BUSINESS
CULTURE
GEAR
IDEAS
SCIENCE
SECURITY

SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

BY ANDY GREENBERG



Hackers wipe US servers of email provider VFEmail

Hackers did not ask for a ransom. VFEmail described the incident as "attack and destroy."

By Catalin Cimpanu for Zero Day | February 12, 2019 -- 10:59 GMT (02:59 PST) | Topic: Security

CIH virus

April, 1998

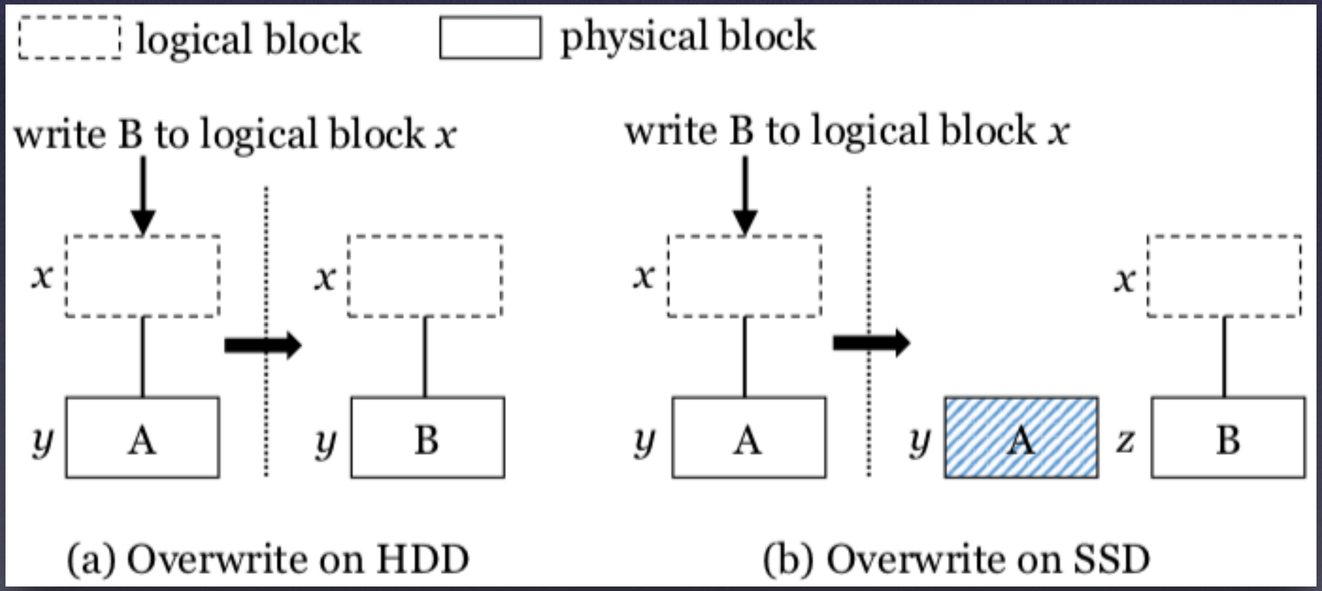
Current solutions

1. backup
2. anti-malware
3. monitor file I/O
4. save encryption keys

FlashGuard (CCS 2017)

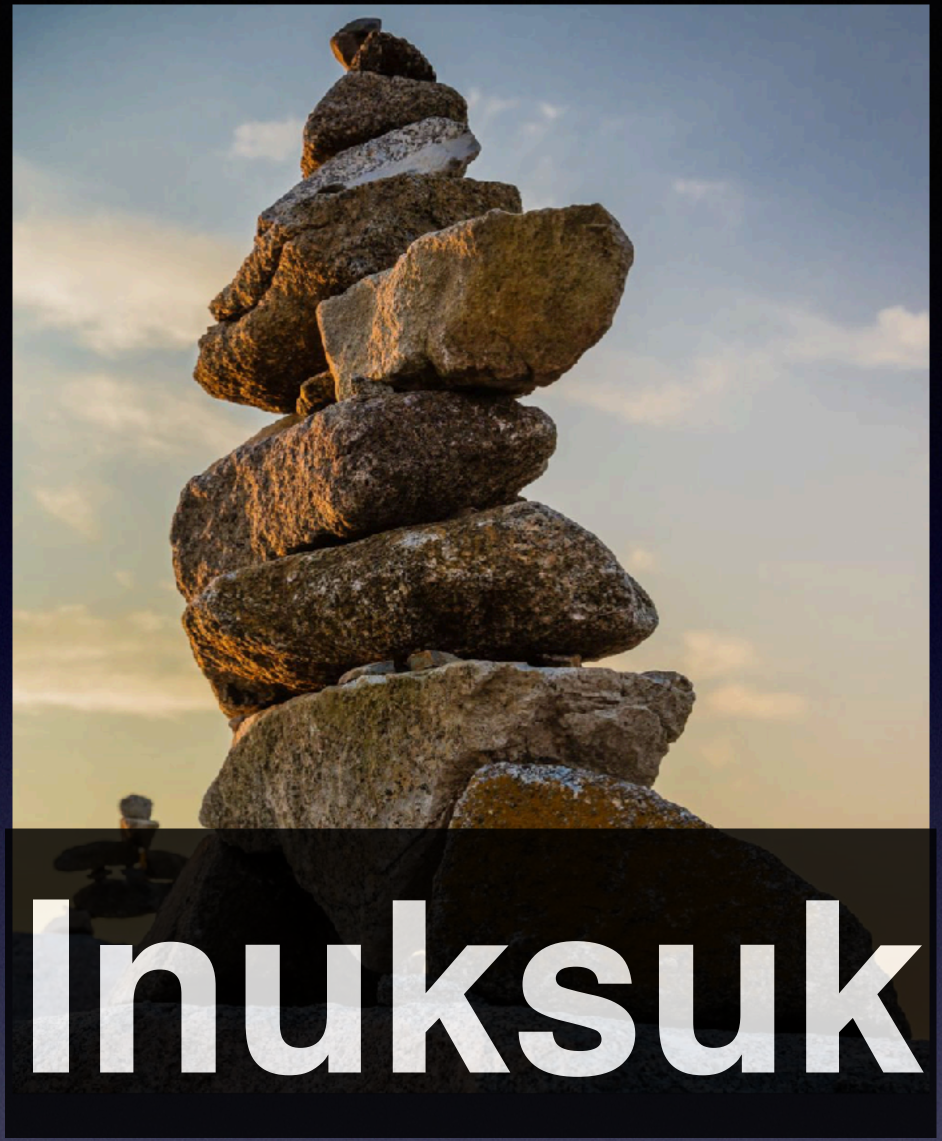
✓ can handle privileged ransomware
✓ relies on intrinsic properties of SSD writes

➡ requires trusted clock, firmware modification
➡ cannot deal with data destruction malware



(a) Overwrite on HDD

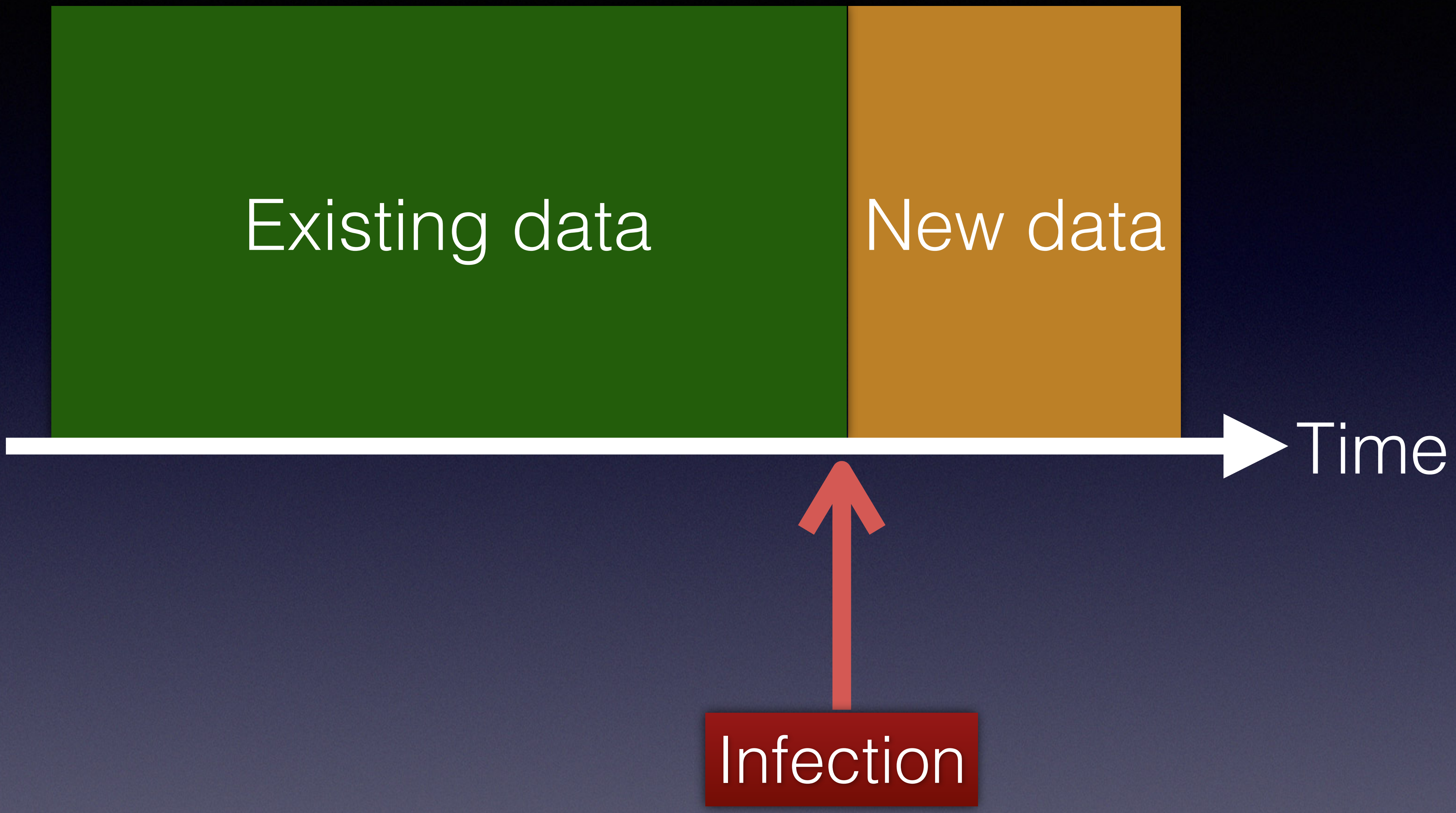
(b) Overwrite on SSD



Inuksuk

Data loss prevention

against privileged malware



Existing data

New data

Time

Infection

We need trusted environments

TEE-Disk: Self-encrypting drives

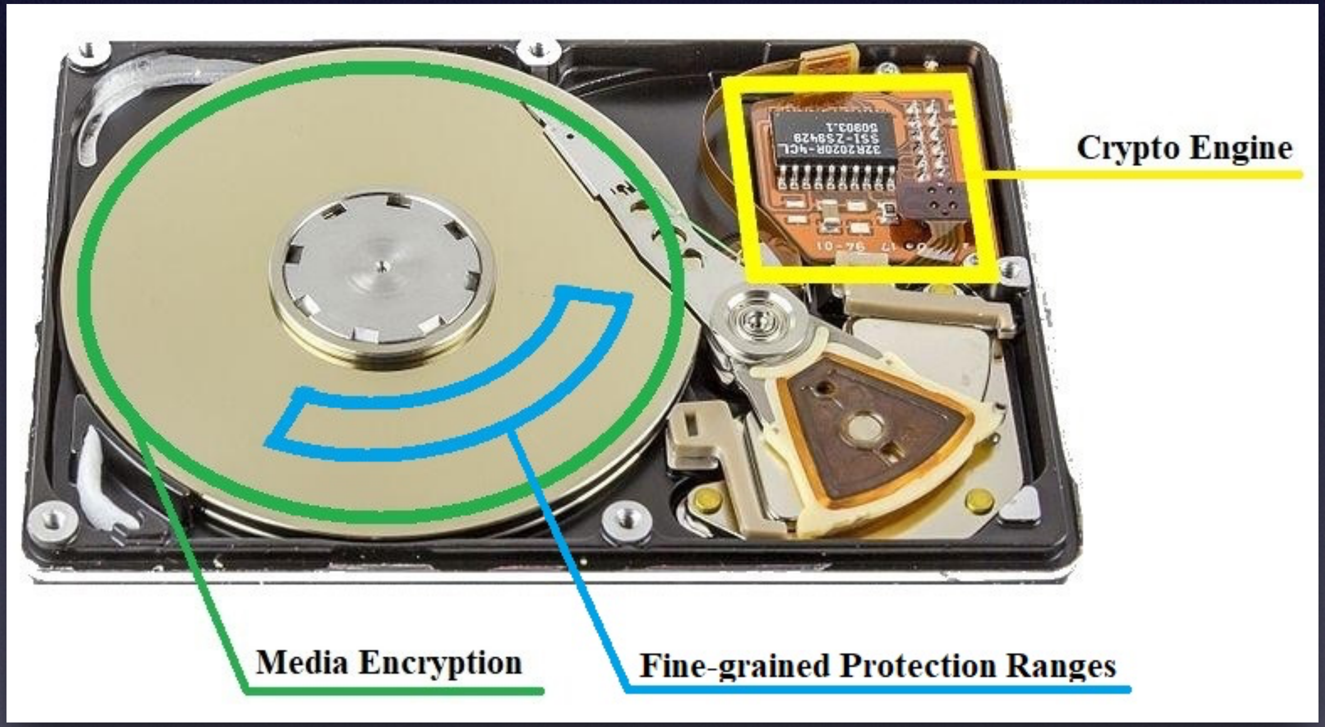
TEE-Host: Intel TXT or AMD SVM

TRUSTED COMPUTING GROUP®

TEE-Disk with:

1. fine-grained **access control**
2. **programmable** control (lock-unlock)

Any SED drive



TEE-Host with:

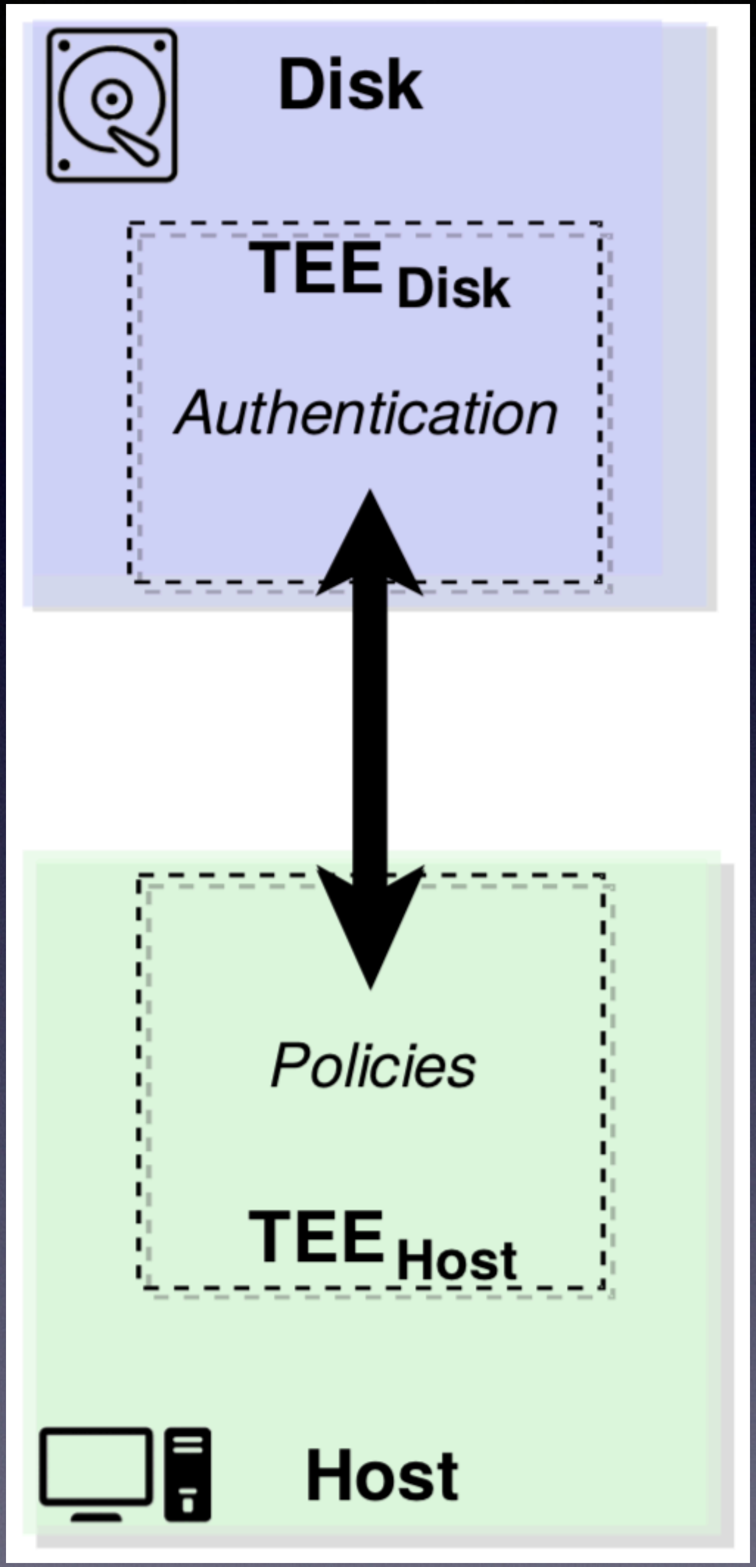
1. dynamic root of trust, isolated
2. sealed secret (platform state binding)
3. device I/O access

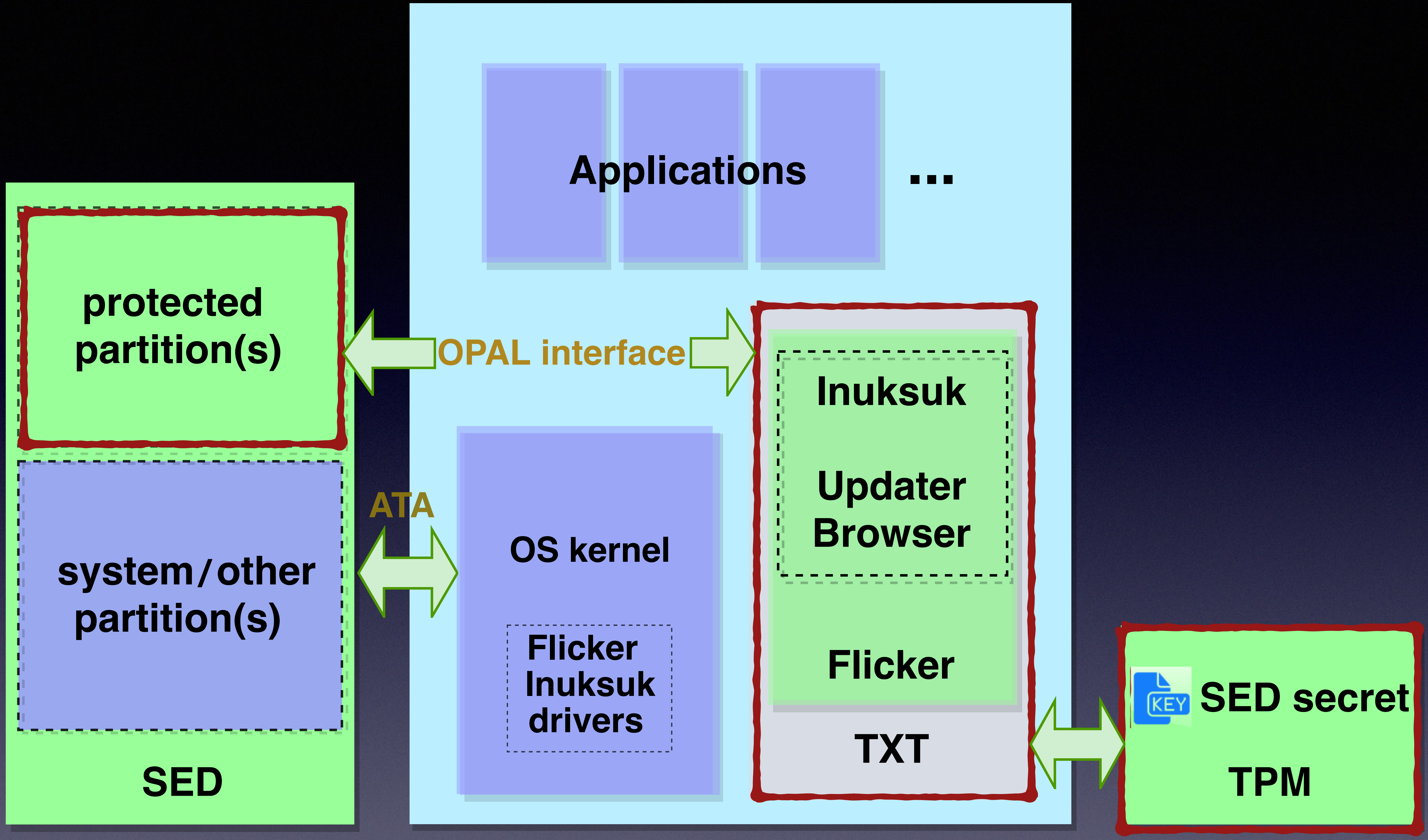
Intel TXT or AMD SVM + a TPM

Design

Read/Recovery: any

Write/Update: authenticated





Applications ...

protected partition(s)

OPAL interface

system/other partition(s)

ATA

OS kernel

Flicker Inuksuk drivers

Inuksuk

Updater Browser

Flicker

TXT

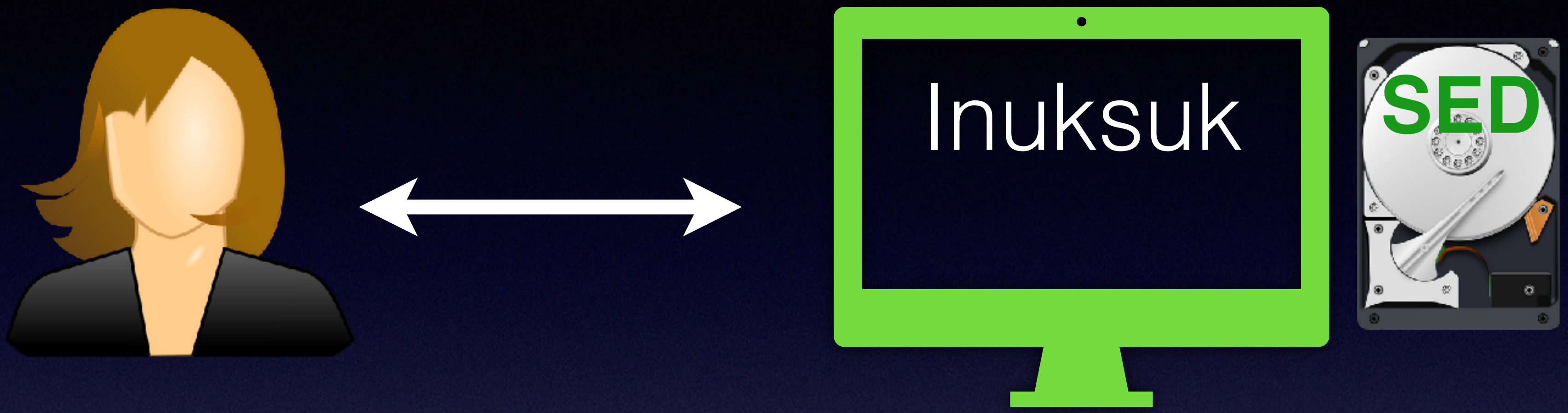
SED

SED secret

TPM

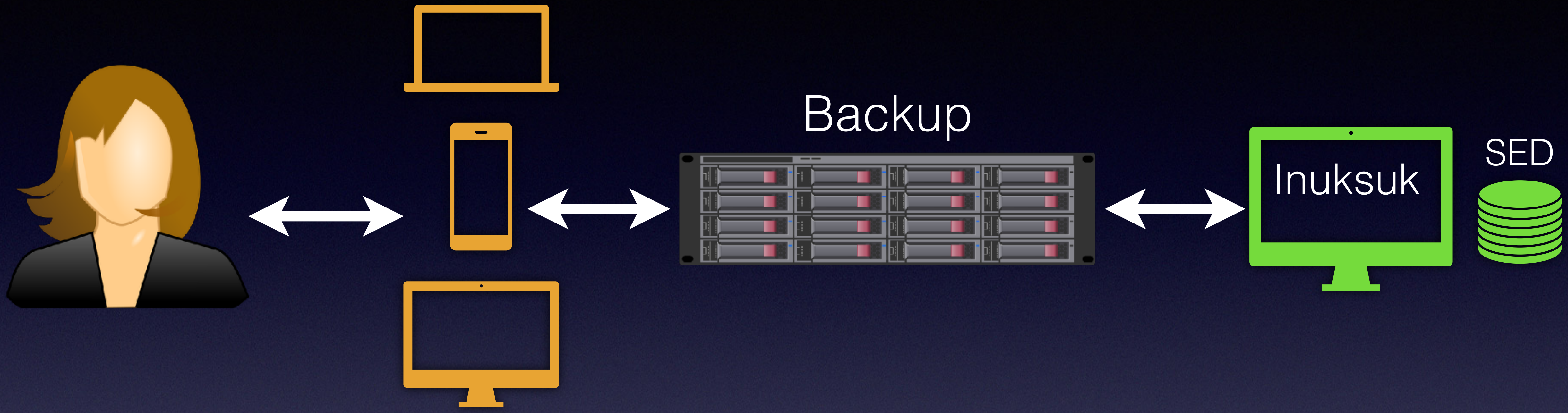
🟦 untrusted 🟩 trusted ▨ TXT coverage

Deployment modes



Stand-alone:

occasional interruptions (TXT exclusiveness)



Network-based:

any user device, no interruptions

Implementation challenges

Windows 7, 10, and Ubuntu (Intel and AMD)

1. Safely use I/O devices from the user OS
2. Programming the SED OPAL interface
3. DMA access in TEE
4. Porting Flicker to Windows 10 64-bit

Performance
(file-transfer: mean MB/sec)

	Write/ Existing	Write/New	Read
50MB file	43.93	41.69	32.17
500KB file	26.46	8.09	16.67

OS and application agnostic, zero penalty

Inuksuk: summary

- Addresses: **wiper** + crypto **ransomware**
- **Rootkit**-capable attacks
- **Multi-TEE** design

Thank you

https://madiba.encs.concordia.ca