PirateShip: Distributed Consensus for (mostly) Trusted Execution Environments

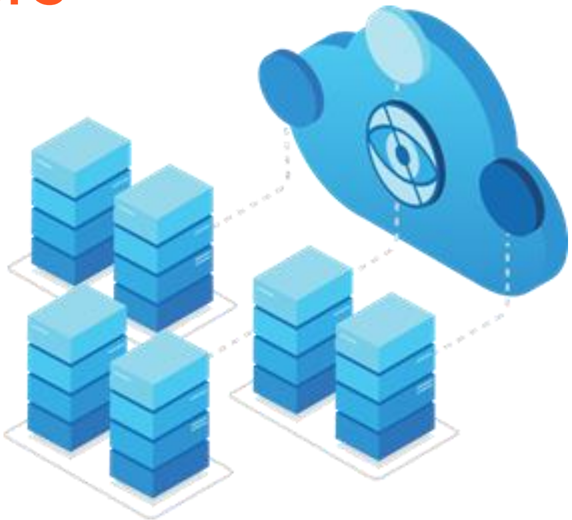
Shubham Mishra, Amaury Chamayou, Natacha Crooks,
Heidi Howard, Markus Kuppe

Context: Distributed Trust Ledgers

Signal

sigstore

HYPERLEDGER INDY

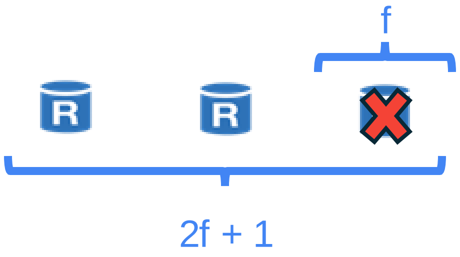


SPLINTER

Hiero

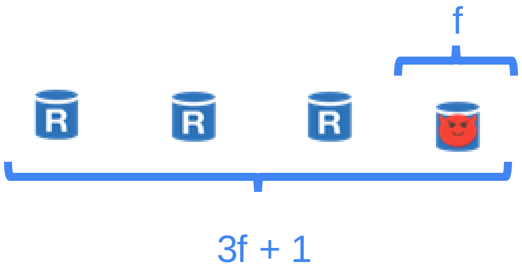
Consensus Protocols

Crash Fault Tolerance (CFT)



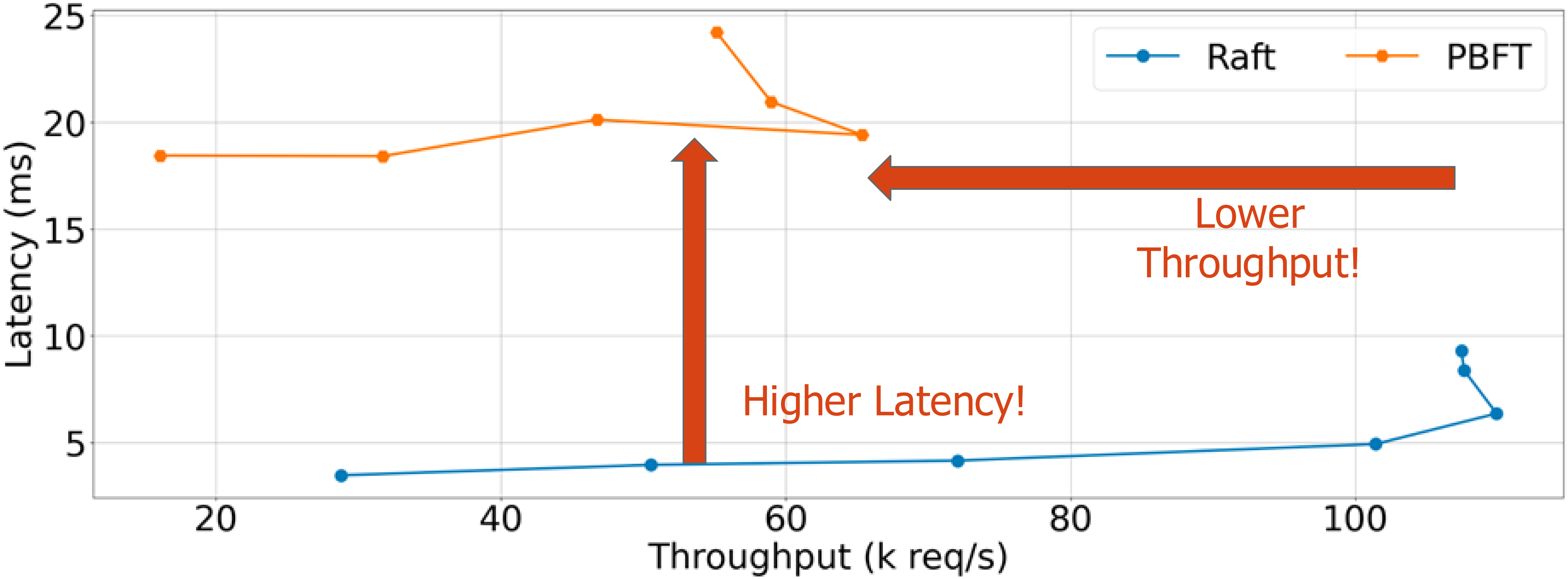
- Must Trust your replicas:
  - Crash,
  - But strictly follow protocol.

Byzantine Fault Tolerance (BFT)



- Replicas not trusted to follow protocol:
  - Arbitrary/malicious behaviour (for at most 1/3rd of nodes)

Why not just use BFT, always?

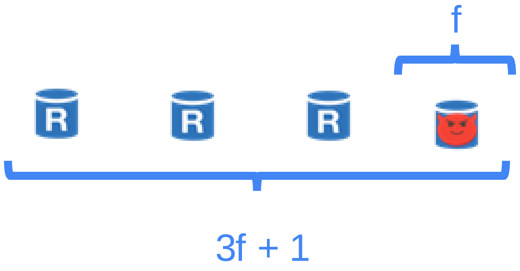


Lower Throughput!

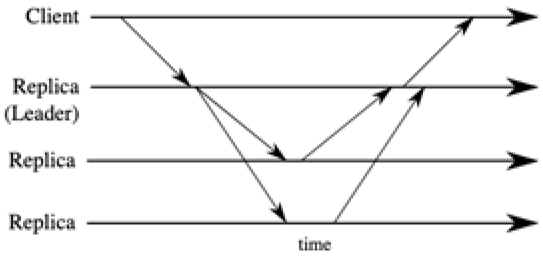
Higher Latency!

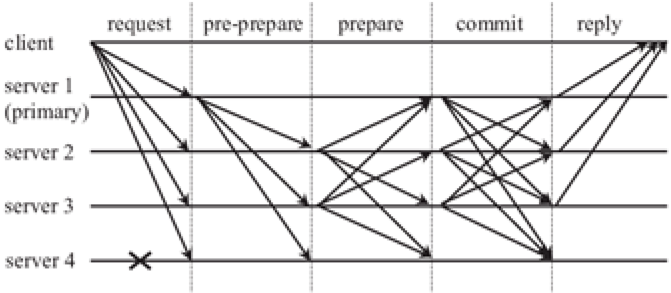
Why?

- f more nodes.



- More phases! (at least 1 more than CFT protocols)





- Crypto overhead:
    - Signatures
    - MACs

Is there a workaround?

Can we STOP malicious behavior from happening?!

Trusted Execution Environments (TEE)

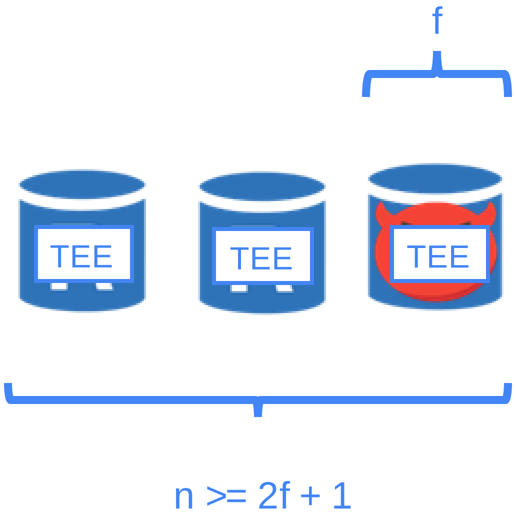
intel TDX

intel SGX

AMD SEV

arm TRUSTZONE

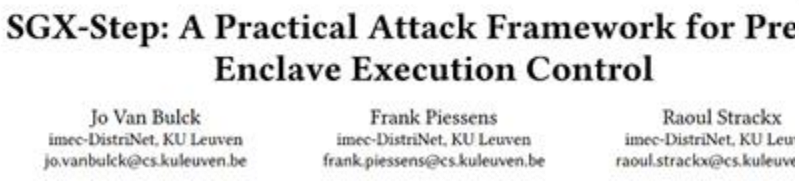
TEEs to rescue



- Integrity
  - Attestation proves to the operator that the code running in each replica is the intended one.
- Confidentiality
  - Hardware protected keys.

Can get away with using cheap CFT protocols! (with some mods)

Are we done?

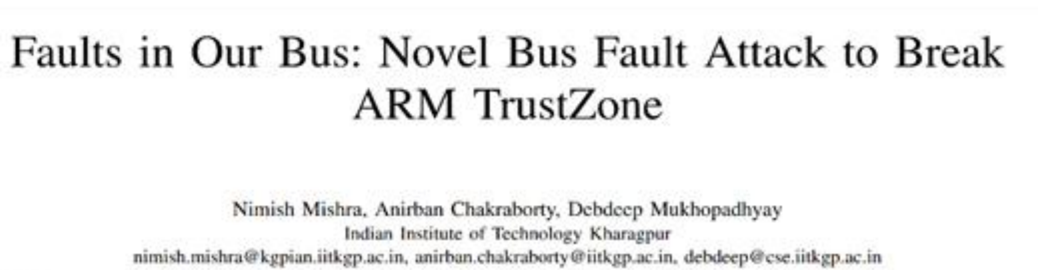


SGX-Step: A Practical Attack Framework for Pre
Enclave Execution Control

Jo Van Bulck
imec-DistriNet, KU Leuven
jo.vanbulck@cs.kuleuven.be

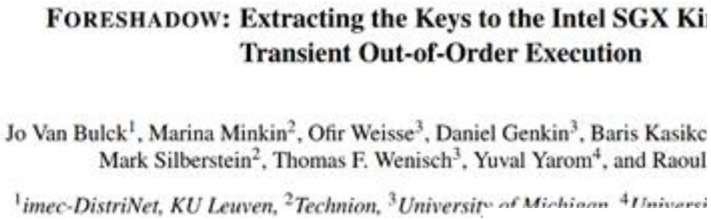
Frank Piessens
imec-DistriNet, KU Leuven
frank.piessens@cs.kuleuven.be

Raoul Strackx
imec-DistriNet, KU Leu
raoul.strackx@cs.kuleuve



Faults in Our Bus: Novel Bus Fault Attack to Break
ARM TrustZone

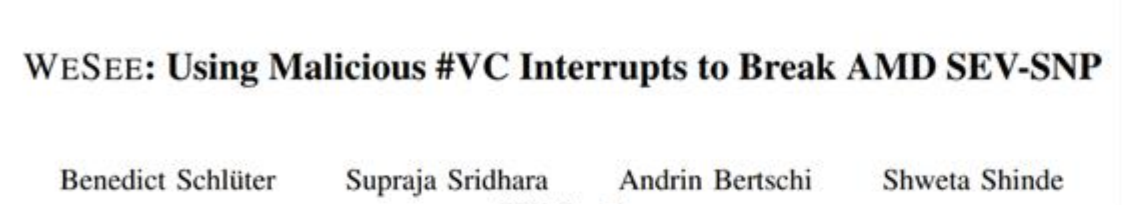
Nimish Mishra, Anirban Chakraborty, Debdeep Mukhopadhyay
Indian Institute of Technology Kharagpur
nimish.mishra@kgpian.iitkgp.ac.in, anirban.chakraborty@iitkgp.ac.in, debdeep@cse.iitkgp.ac.in



FORESHADOW: Extracting the Keys to the Intel SGX Ki
Transient Out-of-Order Execution

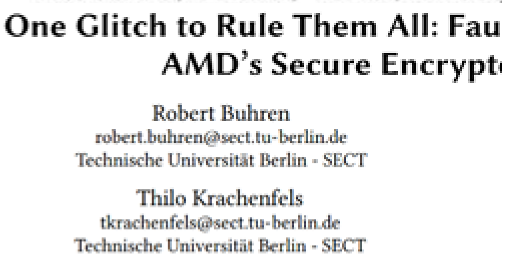
Jo Van Bulck[1], Marina Minkin[2], Ofir Weisse[3], Daniel Genkin[3], Baris Kasikc
Mark Silberstein[2], Thomas F. Wenisch[3], Yuval Yarom[4], and Raoul

[1]imec-DistriNet, KU Leuven, [2]Technion, [3]University of Michigan, [4]Universi



WESEE: Using Malicious #VC Interrupts to Break AMD SEV-SNP

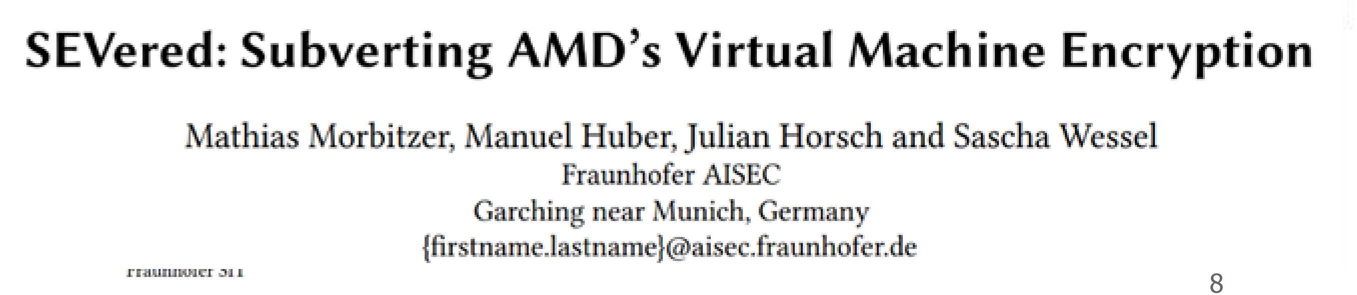
Benedict Schlüter   Supraja Sridhara   Andrin Bertschi   Shweta Shinde



One Glitch to Rule Them All: Fau
AMD's Secure Encrypt

Robert Buhren
robert.buhren@sect.tu-berlin.de
Technische Universität Berlin - SECT

Thilo Krachenfels
tkrachenfels@sect.tu-berlin.de
Technische Universität Berlin - SECT

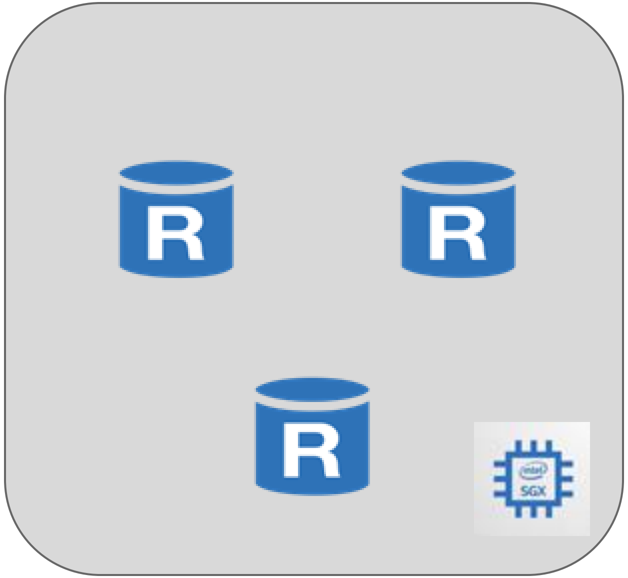


SEVered: Subverting AMD's Virtual Machine Encryption

Mathias Morbitzer, Manuel Huber, Julian Horsch and Sascha Wessel
Fraunhofer AISEC
Garching near Munich, Germany
{firstname.lastname}@aisec.fraunhofer.de

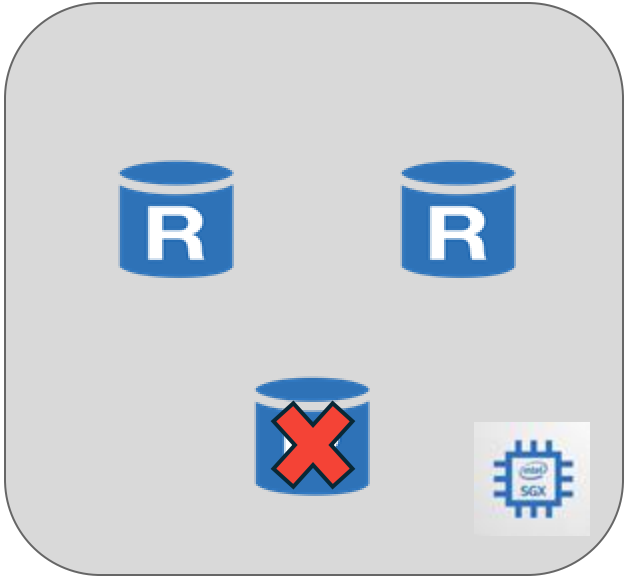
Fraunhofer SIT

What is a realistic model for TEE faults?



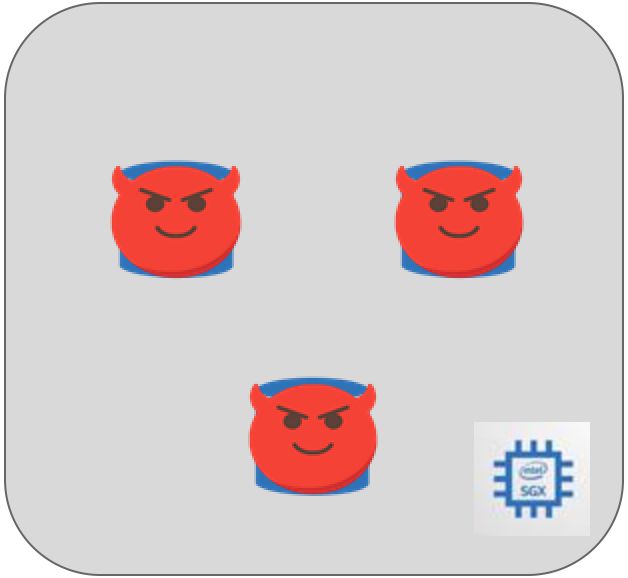
CFT OK!

What is a realistic model for TEE faults?



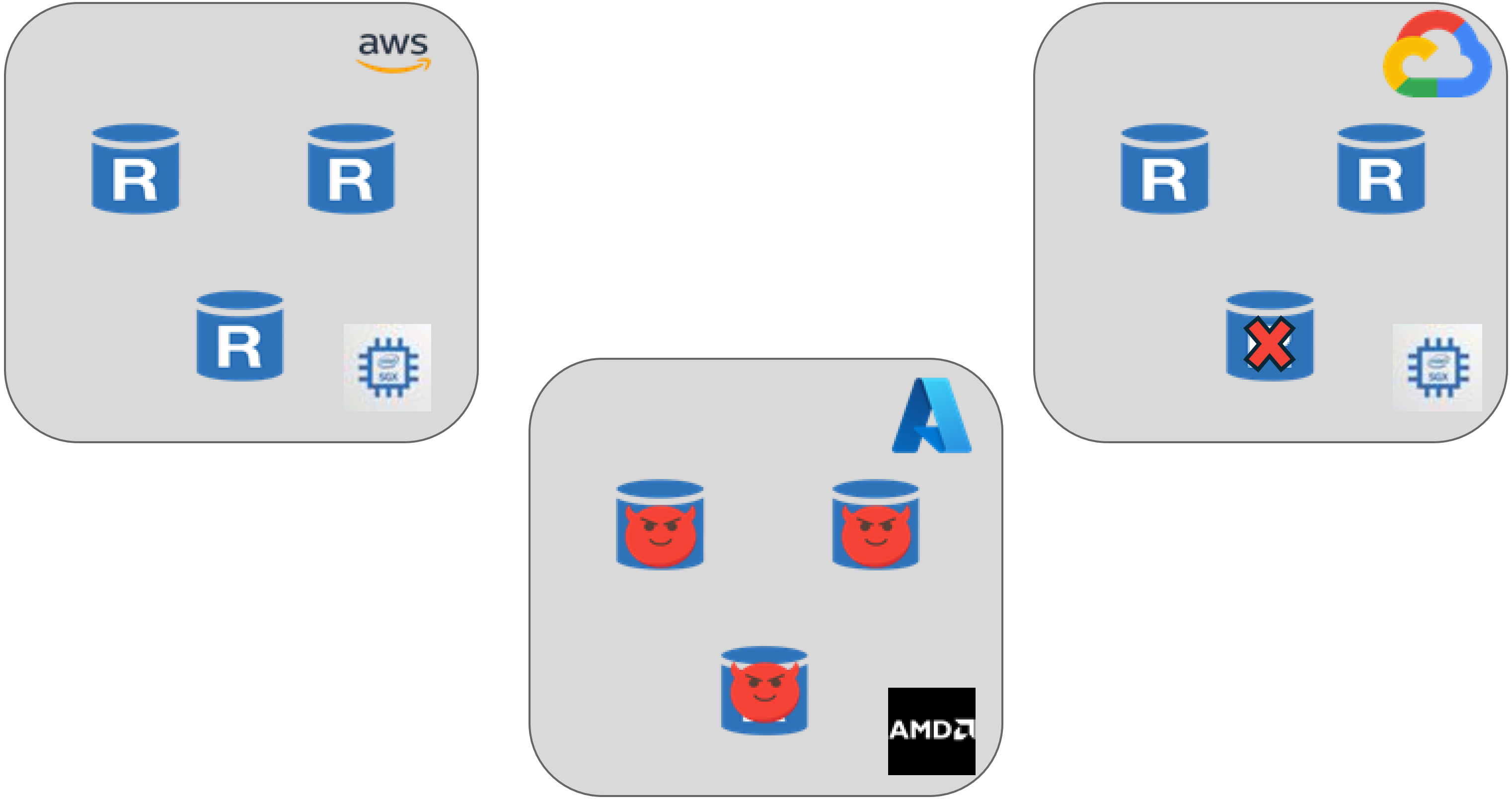
CFT still OK!

What is a realistic model for TEE faults?

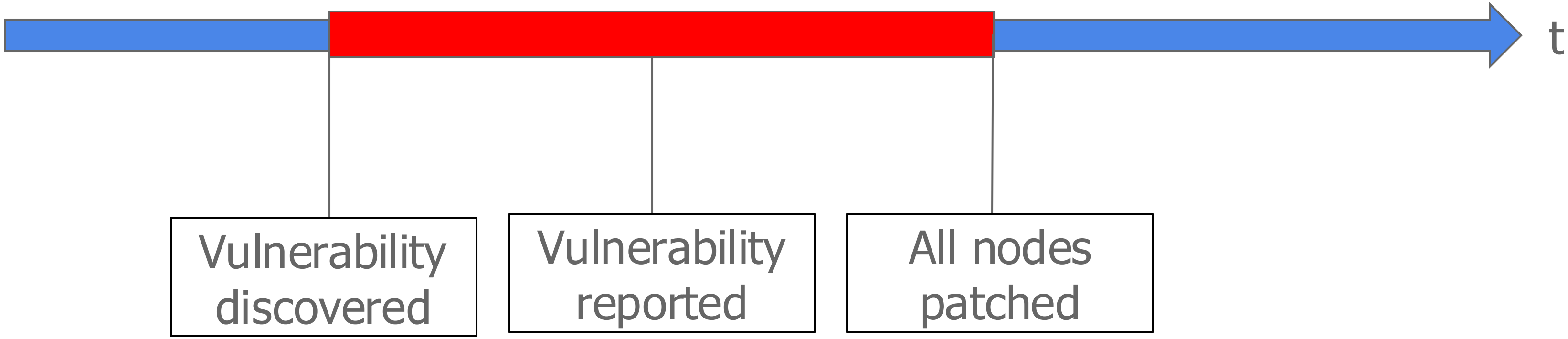


ALL nodes affected!
Even BFT can’t handle this

Platform Fault Tolerance: The better model



Timeline of a TEE platform failure

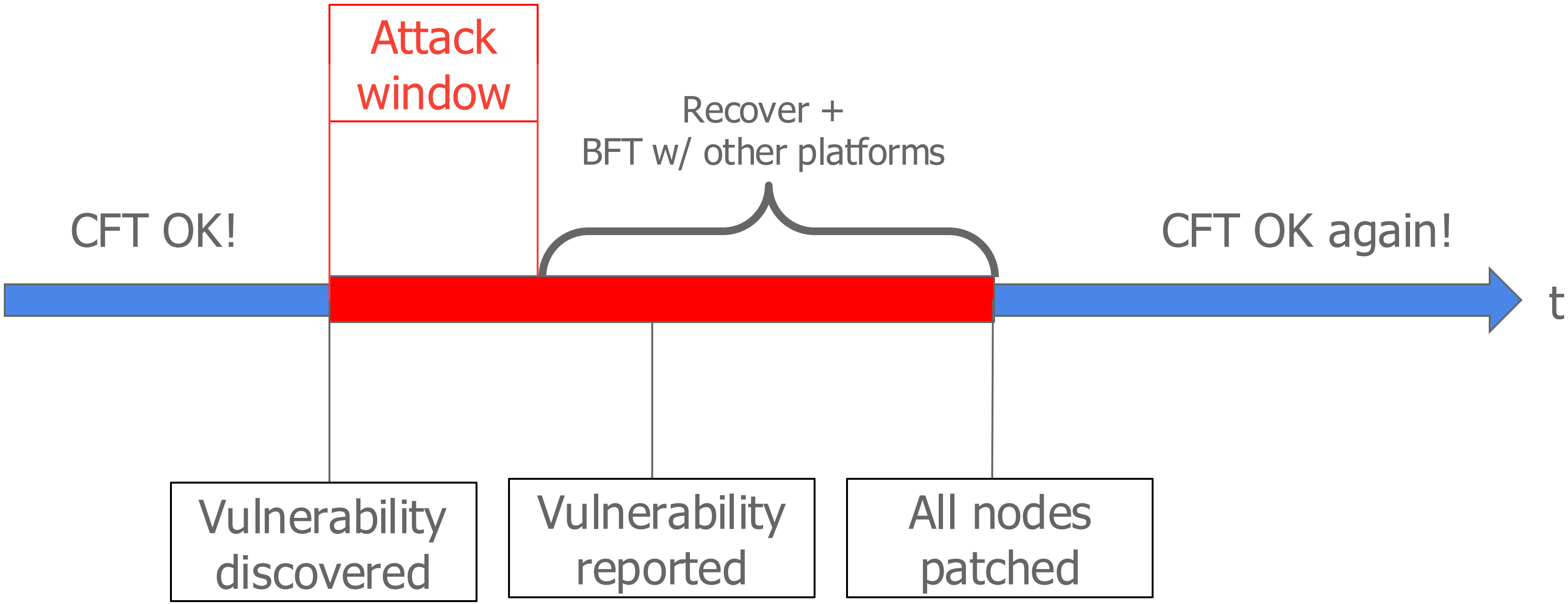


Vulnerability discovered

Vulnerability reported

All nodes patched

Timeline of a TEE platform failure



PirateShip goals

- **Security:** Gracefully handle malicious TEEs/platforms.
  - Quickly check/reconcile logs.
  - Seamless; no external intervention.

- **Performance:** Keep overheads wrt CFT as low as possible.

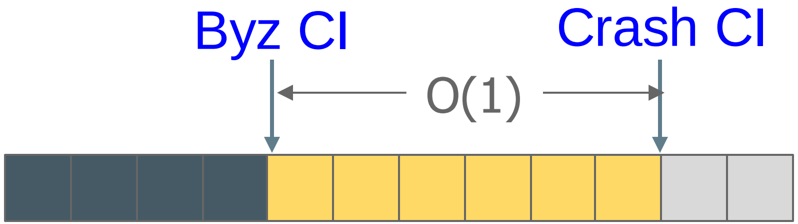
Performance vs Security

Crash Commit

for lower latency

Byz Commit

for better security



Key Idea:

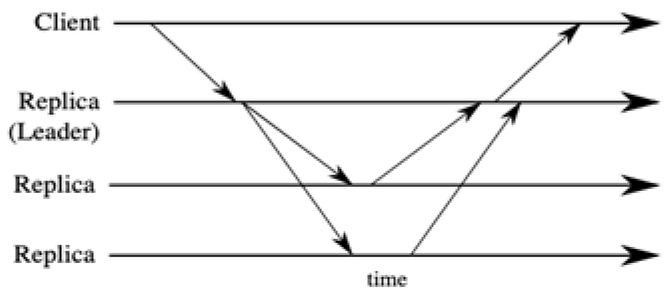
Embedding asynchronous BFT logic inside CFT protocol

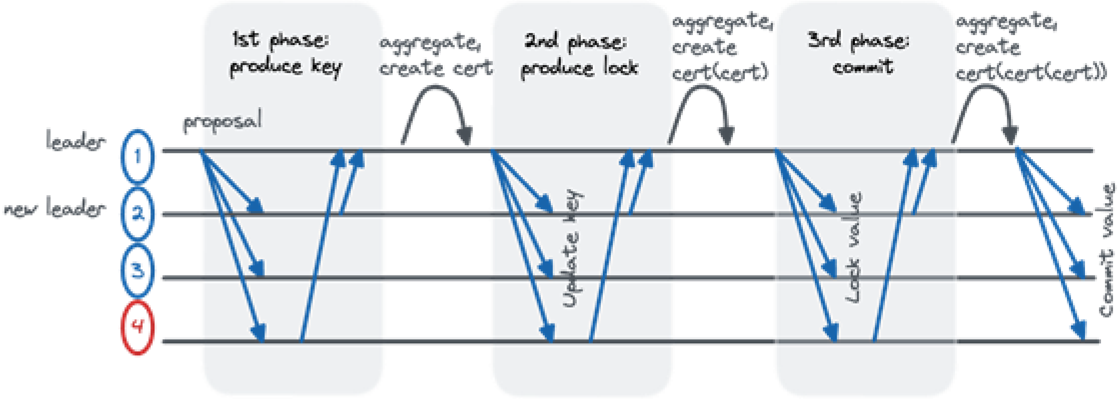
without sending extra messages

How?

Key Insight:

CFT and BFT protocols are not THAT different!

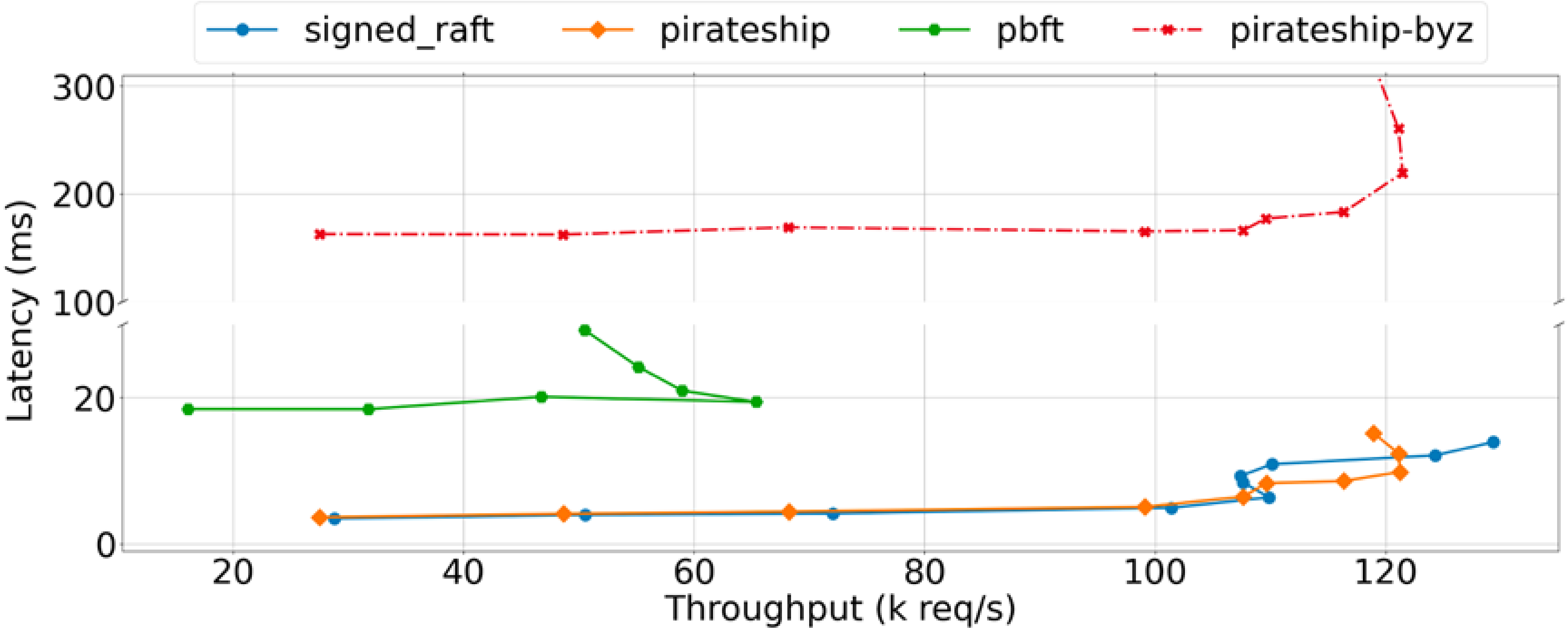




How?

- Pipelining
- Hash-chaining
- Asynchronous vote counting

Initial Results



Conclusion

- We present the notion of Platform Fault Tolerance to better model TEE-based distributed ledgers.
- We presented PirateShip, a new consensus protocol for TEEs that exhibits CFT-like performance but asynchronously provides BFT guarantees.

Thank you!

Questions?

shubham_mishra@berkeley.edu