CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Forking Attacks on SGX Applications are Real

Annika Wilde, Samira Briongos, Claudio Soriente, Ghassan Karame

RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

HORST GÖRTZ INSTITUT

TALK OUTLINE

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

1. Introduction
2. Forking Attacks & Mitigations
3. Study
4. Discussion
5. Summary & Outlook

ABOUT ME

- Annika Wilde

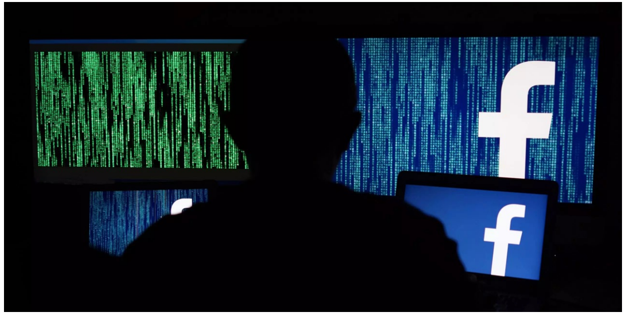
- Chair for Information Security at Ruhr-University Bochum
- PhD student since October 2022

- Research:
  - Platform Security
  - Trusted Execution Environments (SGX, Keystone)

CLOUD COMPUTING

Facebook hack April 2021 [1]

- Database exposed in plain
- 530 million users affected



➔ Trusted Execution Environments (TEE)

- ARM TrustZone (Samsung, Huawei, …)
- Intel SGX (Signal, …)

[1] https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

INTEL SECURE GUARD EXTENSION (SGX)

- Extension of the x86 ISA
- Hardware-based isolation for trusted code – *enclaves*
- Trusted runtime memory
- Sealing: persist enclave state across enclave restarts
    - Encrypt data with a platform-specific key
- Attestation: verifiable certificate of enclave code + platform

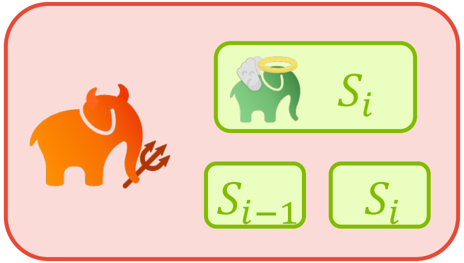
Forking Attacks & Mitigations

FORKING ATTACKS

Rollback

Problem:

Enclaves ensure the **confidentiality and integrity** of sealed data, BUT enclaves cannot verify **freshness**



FORKING ATTACKS

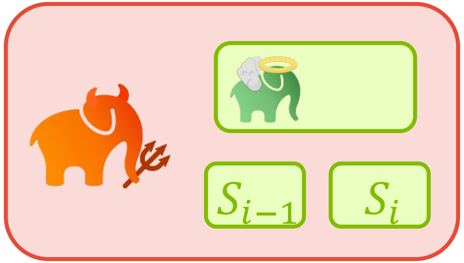
Rollback

Problem:

Enclaves ensure the **confidentiality and integrity** of sealed data, BUT enclaves cannot verify **freshness**

Attack:

1. The attacker terminates the enclave



FORKING ATTACKS

Rollback

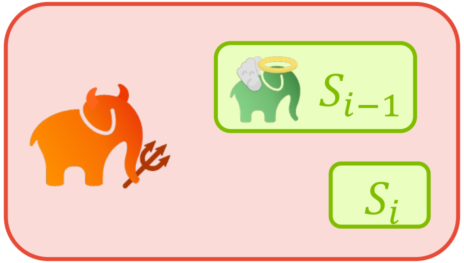
Problem:

Enclaves ensure the **confidentiality and integrity** of sealed data, BUT enclave cannot verify **freshness**

Attack:

1. The attacker terminates the enclave
2. The attacker provides a stale state

➔ The enclave initializes to a stale state



FORKING ATTACKS

Cloning

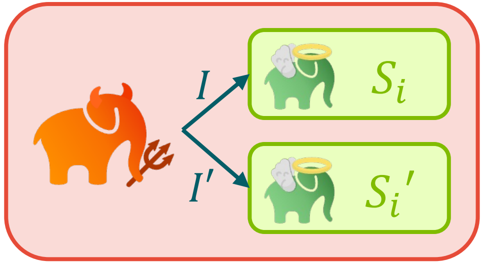
Problem:

Enclaves cannot determine the **number of instances** running on a machine

Attack:

1. The attacker launches n instances of the enclave
2. The enclaves have the same ID
3. The attacker provides different inputs

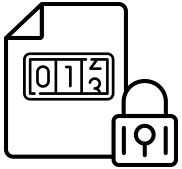
➔ Diverging enclave states



FORKING MITIGATIONS

Monotonic Counters

- Counter strictly increasing



Rollback:
- Sealing: increase MC + seal it
- Unsealing: verify sealed MC

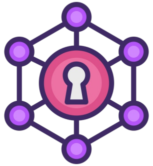
Cloning:
- Increase MC on enclave start
- Periodically check MC value

Trusted Third Party

- External party tracking the enclave state

Distributed Systems

- Distributed system tracking state
- Components secure each other's state
- Fault tolerance mechanisms



FORKING MITIGATIONS

CloneBuster [2]

- Use cache as a covert channel
- Enclaves self-detect if they are cloned

- No rollback protection
- Cloning protection without TTP

➔ Secure enclaves that do not seal state

[2] No Forking Way: Detecting Cloning Attacks on Intel SGX Applications, Briongos *et al.*, 2023

FORKING MITIGATIONS

CloneBuster [2]

19%
SGX-based applications are vulnerable to cloning attacks

[2] No Forking Way: Detecting Cloning Attacks on Intel SGX Applications, Briongos *et al.*, 2023

CASA
Cyber Security in the Age of Large-Scale Adversaries

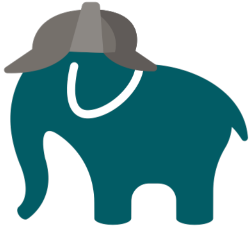
Study

Impact of Cloning Attacks

CASA
Cyber Security in the Age of Large-Scale Adversaries

Research question:

How big is the impact of cloning attacks?



COLLECTION OF APPLICATIONS

- sgx-papers [3]
- Awesome SGX Open Source Projects [4]

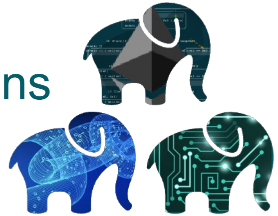
Excluding:
- Libraries
- Runtime frameworks
- Projects without design documentation

[3] https://github.com/vschiavoni/sgx-papers
[4] https://github.com/Maxul/Awesome-SGX-Open-Source

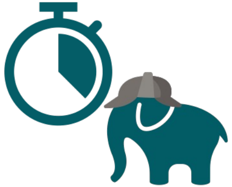
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

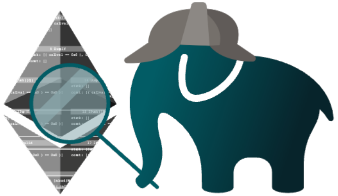
APPLICATION ANALYSIS

72 applications



~ 2 hours per application





Manual investigation

150 hours in total

APPLICATION ANALYSIS

Example

Application:

- Aria [5]
- IEEE ICDE 2021
- In-memory KVS
- Encrypted storage
- Enclave manages encryption keys

Analysis:

1. Is source code available? → No
2. Is the application vulnerable to rollback attacks? → No
3. Is the application susceptible to cloning attacks? → Yes

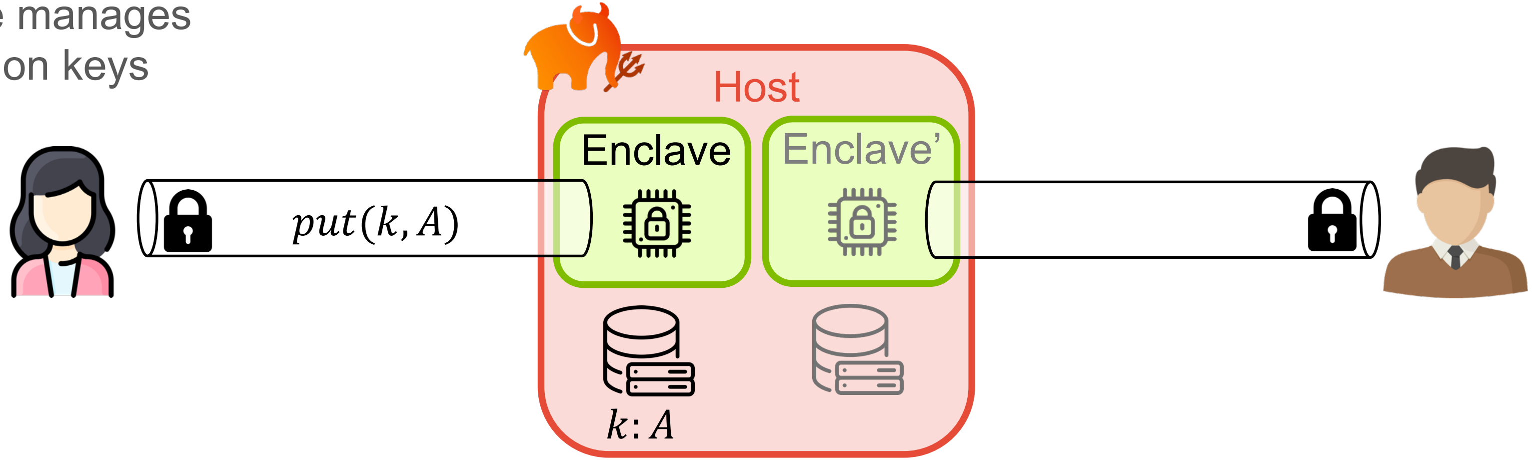
[5] Aria: Tolerating Skewed Workloads in Secure In-memory Key-value Stores, Yang *et al.*, 2021

APPLICATION ANALYSIS

Exemplary Attack

Aria [5]

- In-memory KVS
- Encrypted storage
- Enclave manages encryption keys



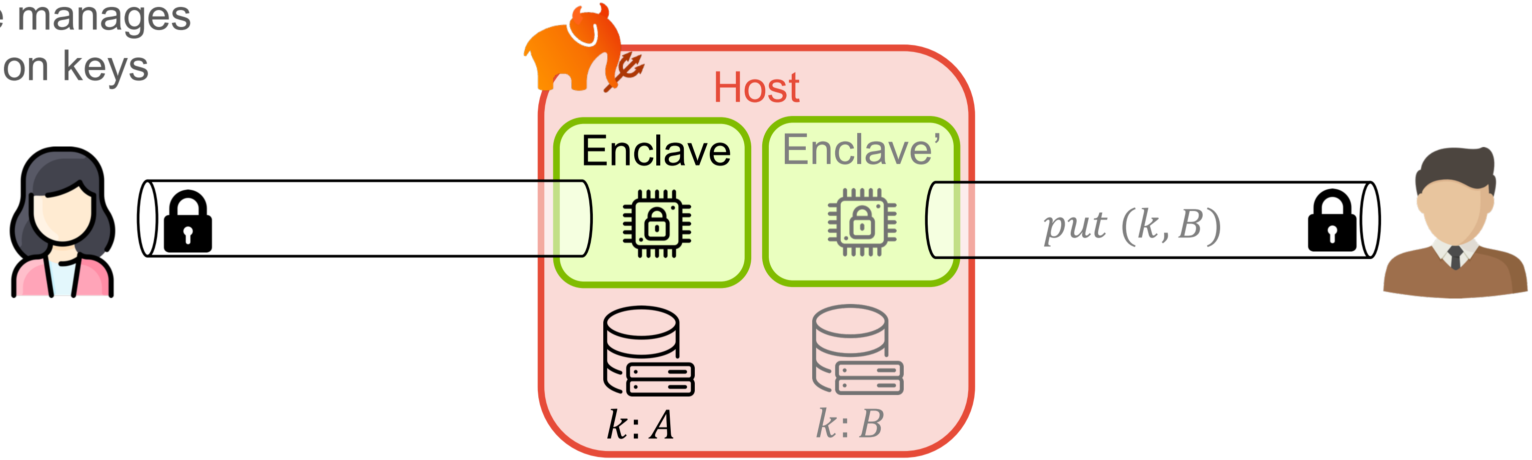
[5] Aria: Tolerating Skewed Workloads in Secure In-memory Key-value Stores, Yang *et al.*, 2021

APPLICATION ANALYSIS

Exemplary Attack

Aria [5]

- In-memory KVS
- Encrypted storage
- Enclave manages encryption keys



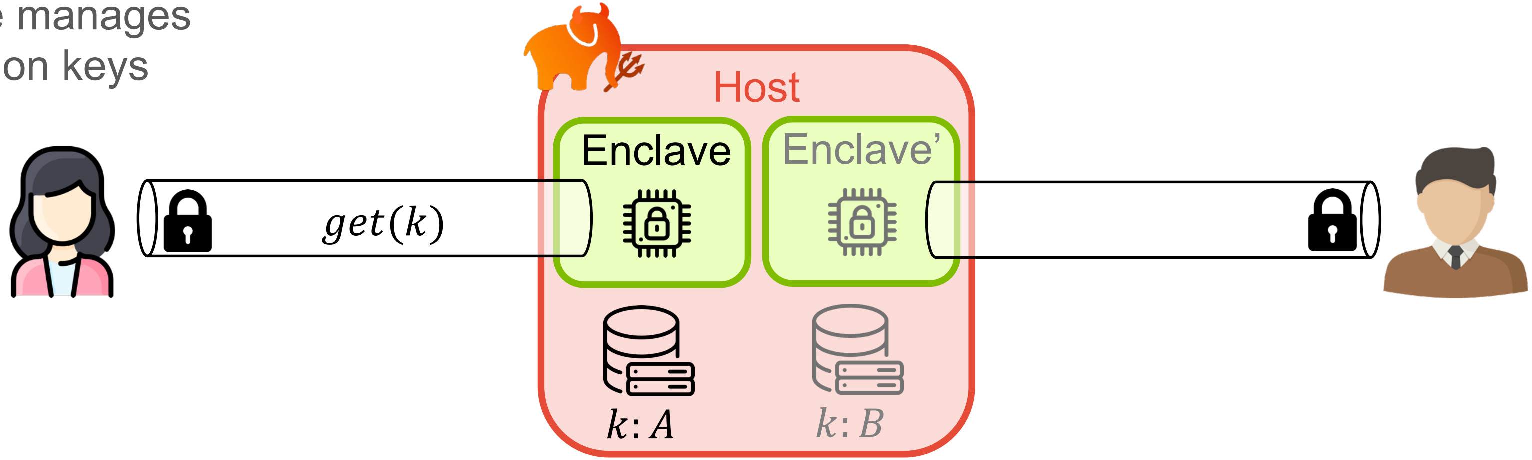
[5] Aria: Tolerating Skewed Workloads in Secure In-memory Key-value Stores, Yang *et al.*, 2021

APPLICATION ANALYSIS

Exemplary Attack

Aria [5]

- In-memory KVS
- Encrypted storage
- Enclave manages encryption keys



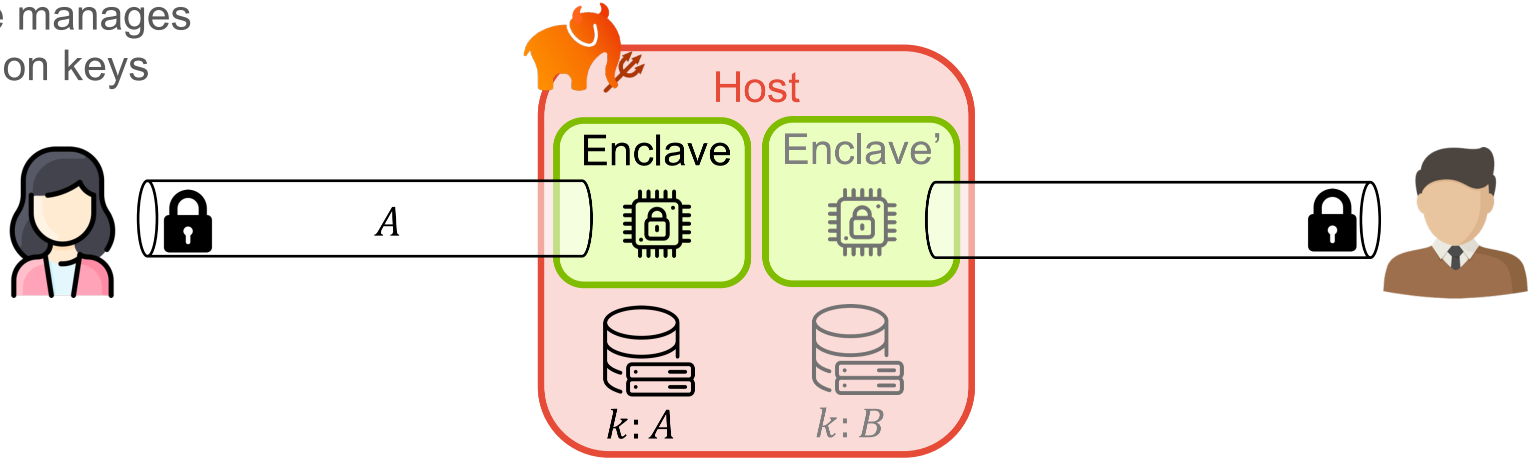
[5] Aria: Tolerating Skewed Workloads in Secure In-memory Key-value Stores, Yang *et al.*, 2021

APPLICATION ANALYSIS

Exemplary Attack

Aria [5]

- In-memory KVS
- Encrypted storage
- Enclave manages encryption keys



[5] Aria: Tolerating Skewed Workloads in Secure In-memory Key-value Stores, Yang *et al.*, 2021

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CHALLENGES

- Ambiguous design documentation
  - How exactly are forking mitigations used?
  - How is the enclave interface defined?
  - …
- Missing implementation
- Incomplete implementation
- Blockchain applications
  - Can cloning attacks circumvent consensus?

KEY OBSERVATIONS

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Observation 1: 19% of the applications are vulnerable to cloning attacks.

Observation 2: All vulnerable applications can be assigned to one of 3 attack categories.

Observation 3: Database applications are particularly vulnerable.

Observation 4: 51% of the applications lack design documentation.

Observation 5: 25% of the applications provide no source code.

Observation 6: 33% of the applications provide incomplete implementations.

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Thank you :)

RUHR-UNIVERSITÄT BOCHUM
Horst-Görtz-Institut für IT-Sicherheit
Exzellenzcluster CASA
MC 0.75 | Universitätsstr. 150 | 44780 Bochum | Germany
www.casa.rub.de | www.hgi.rub.de

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM RUB

HGI HORST GÖRTZ INSTITUT