Horizontal Privilege Escalation in Trusted Applications

Darius Suciu Stephen McLaughlin Laurent Simon Radu Sion

Stony Brook University
Computer Science Department

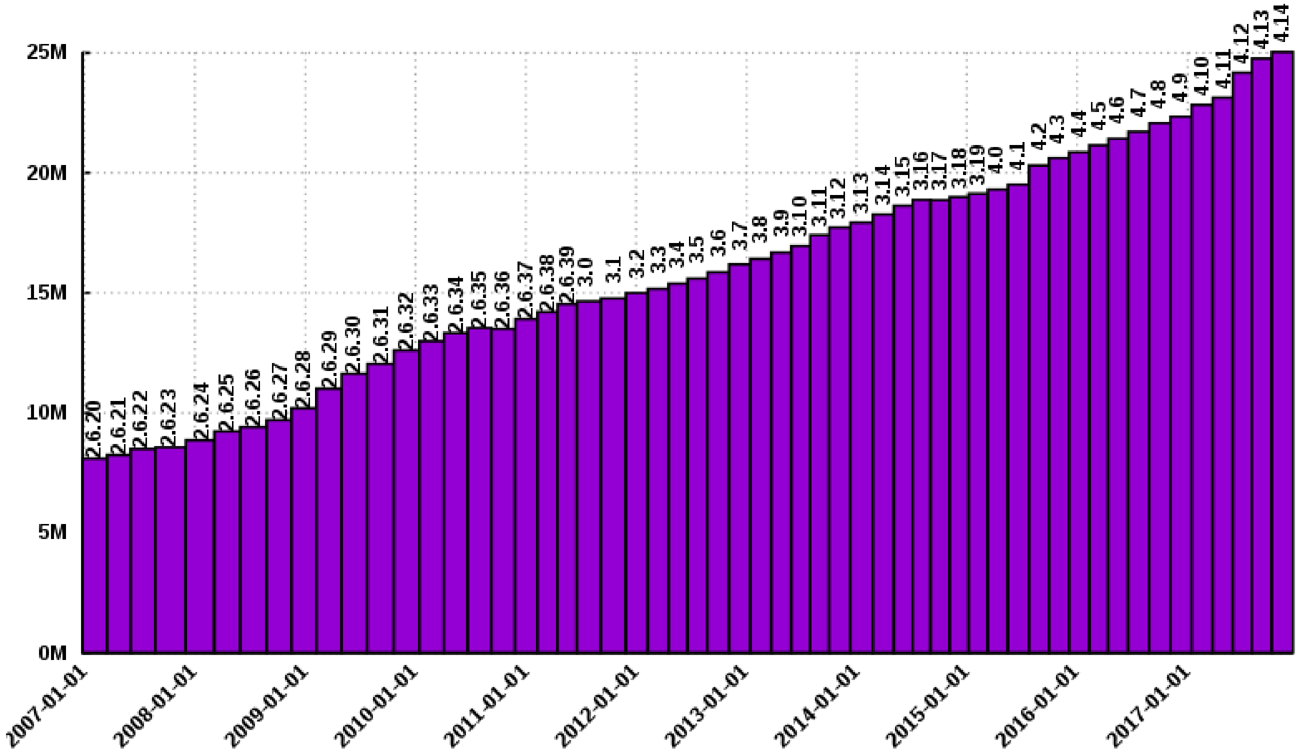
Office of Naval Research
Science & Technology

NSi
National Security Institute

SAMSUNG
RESEARCH AMERICA

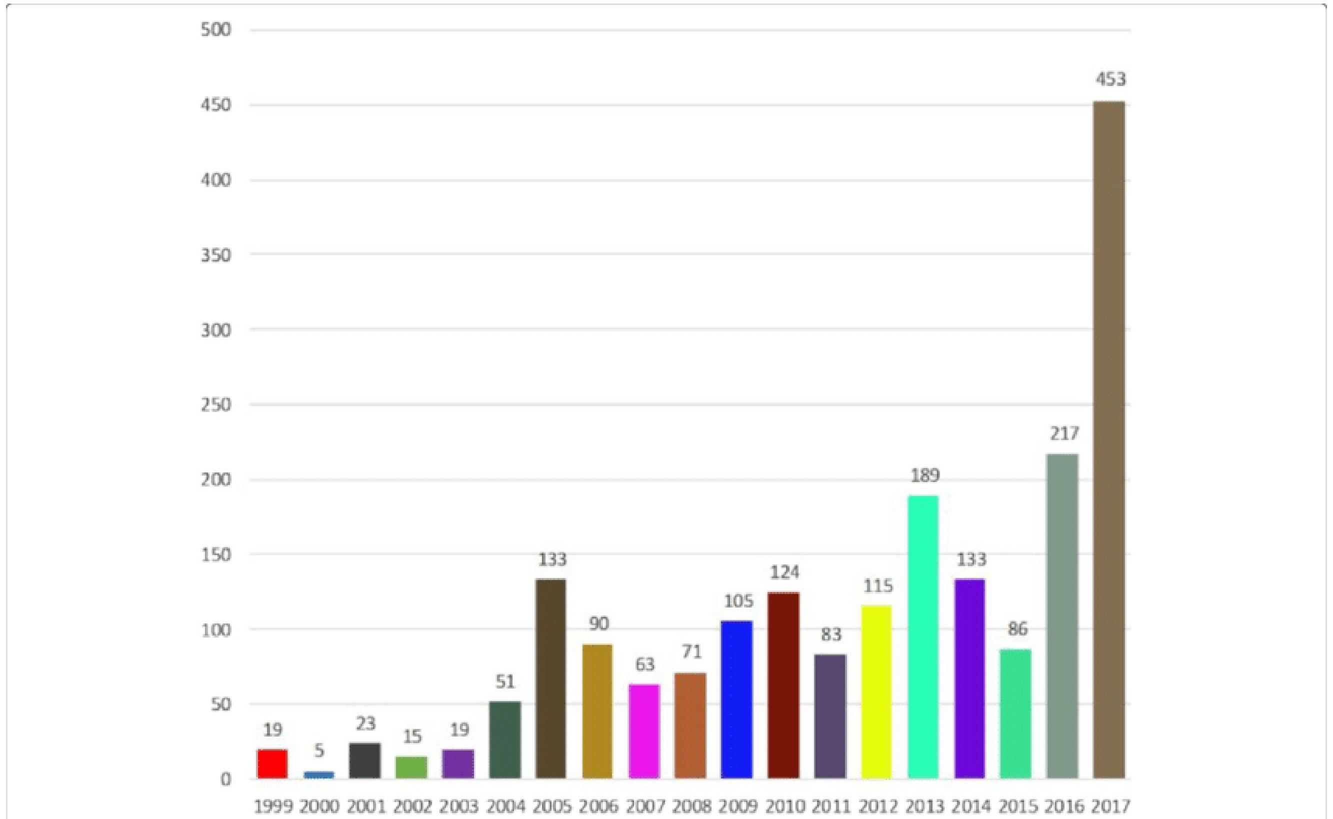
Background: Bugs over time

Linux lines of code over time



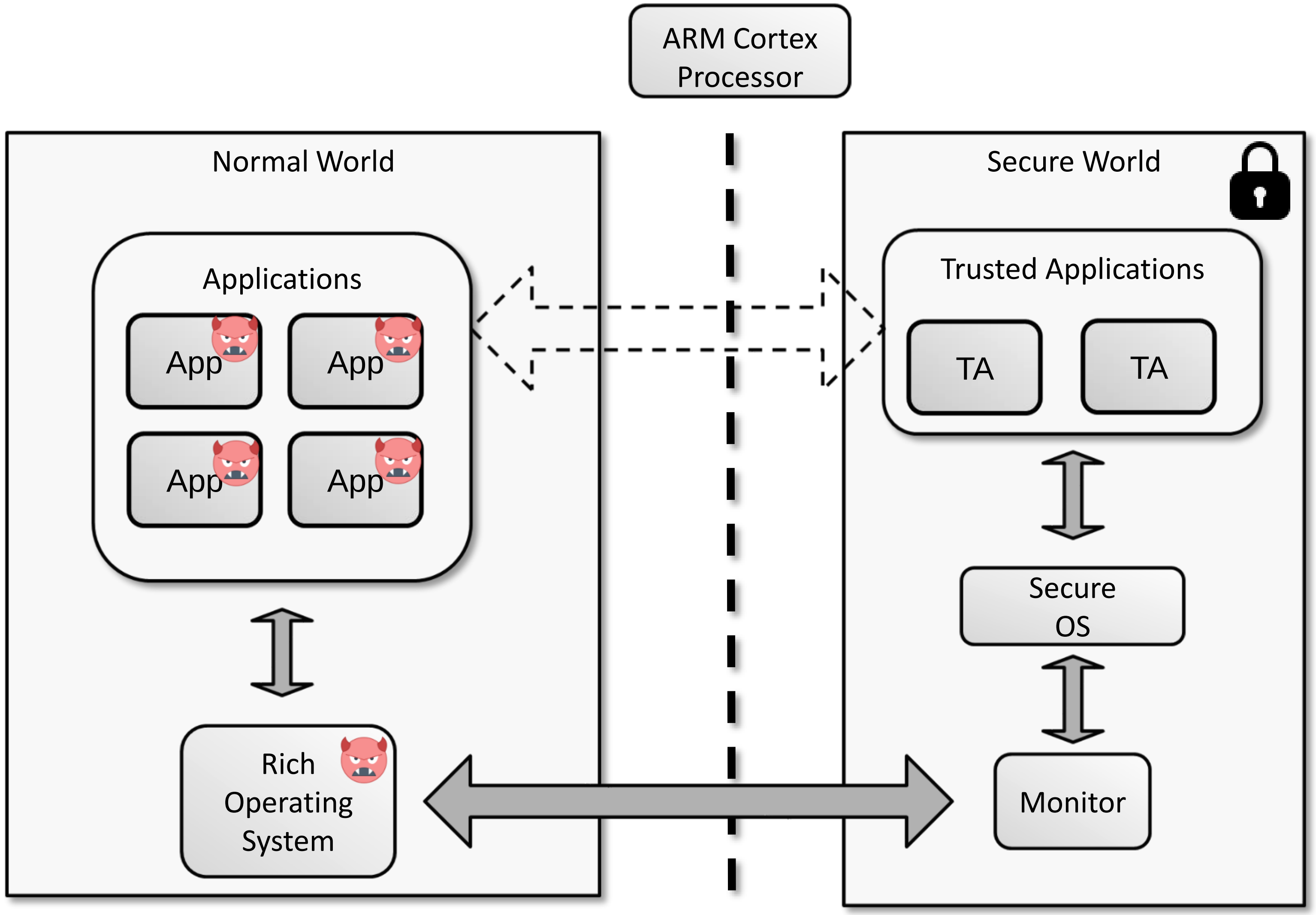
Source: https://commons.wikimedia.org/wiki/File:Lines_of_Code_Linux_Kernel.svg

Linux vulnerabilities over time

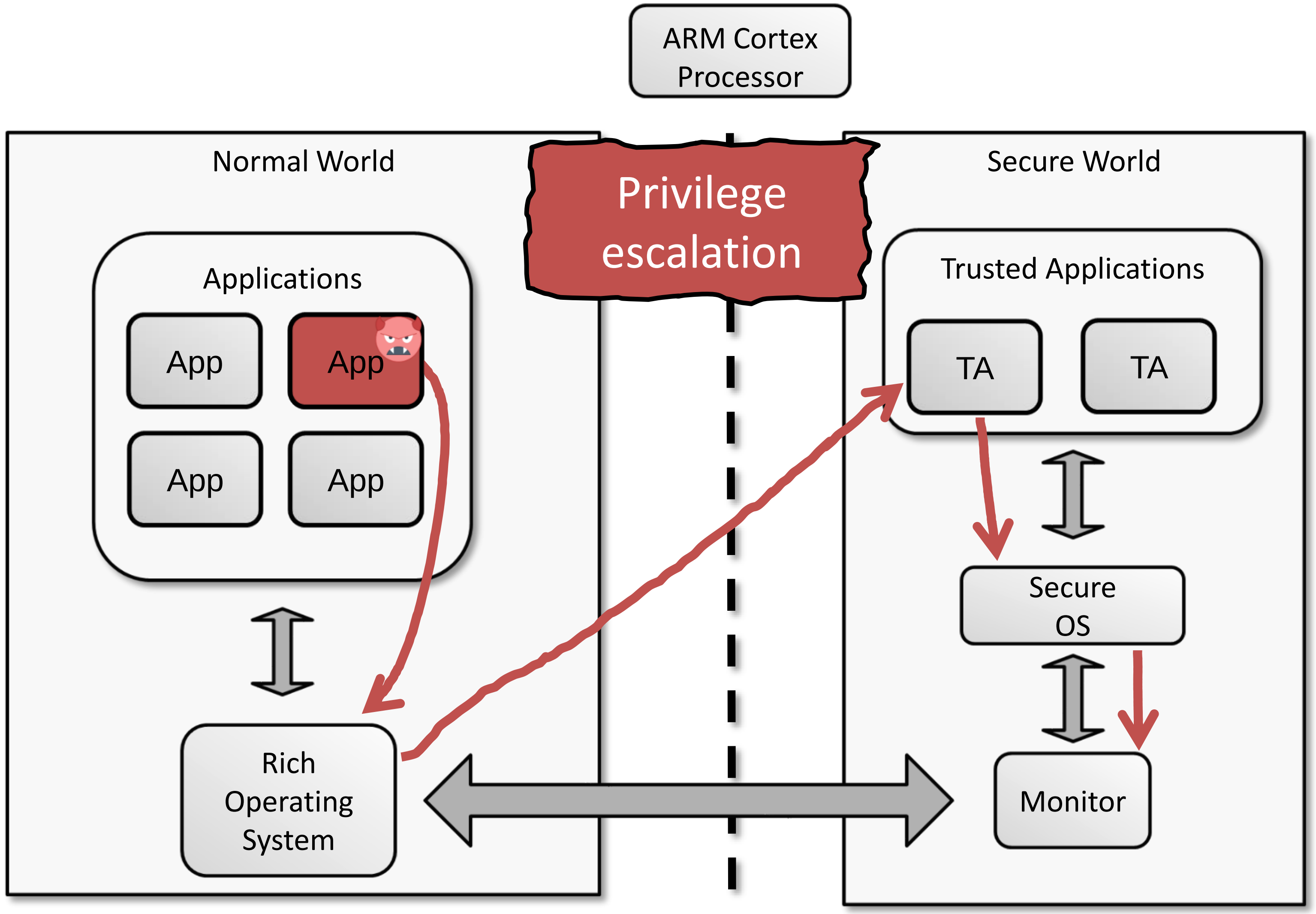


Source: Meng, Dan, et al. "Security-first architecture: deploying physically isolated active security processors for safeguarding the future of computing."

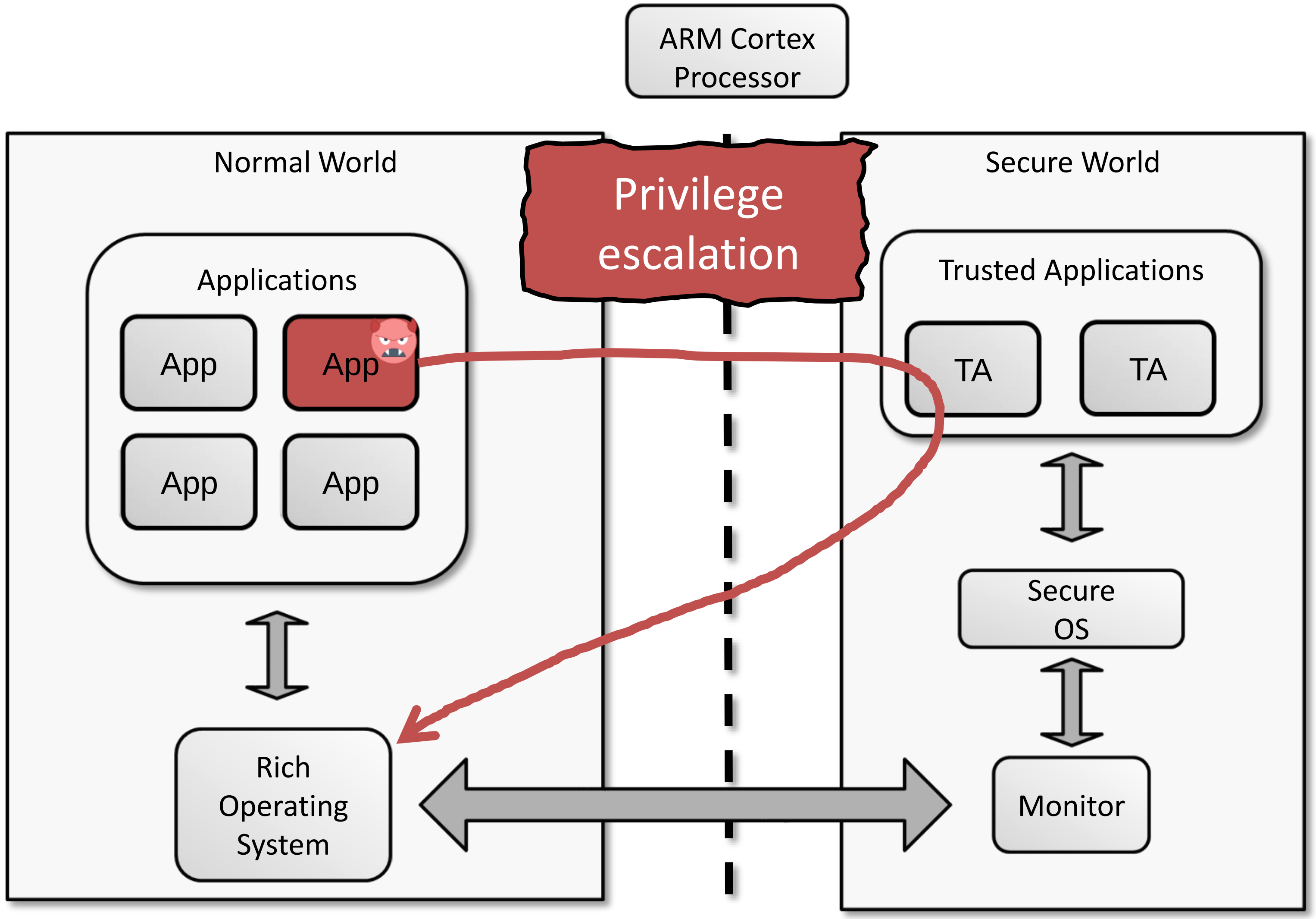
Background: TrustZone



Background: TrustZone Attacks

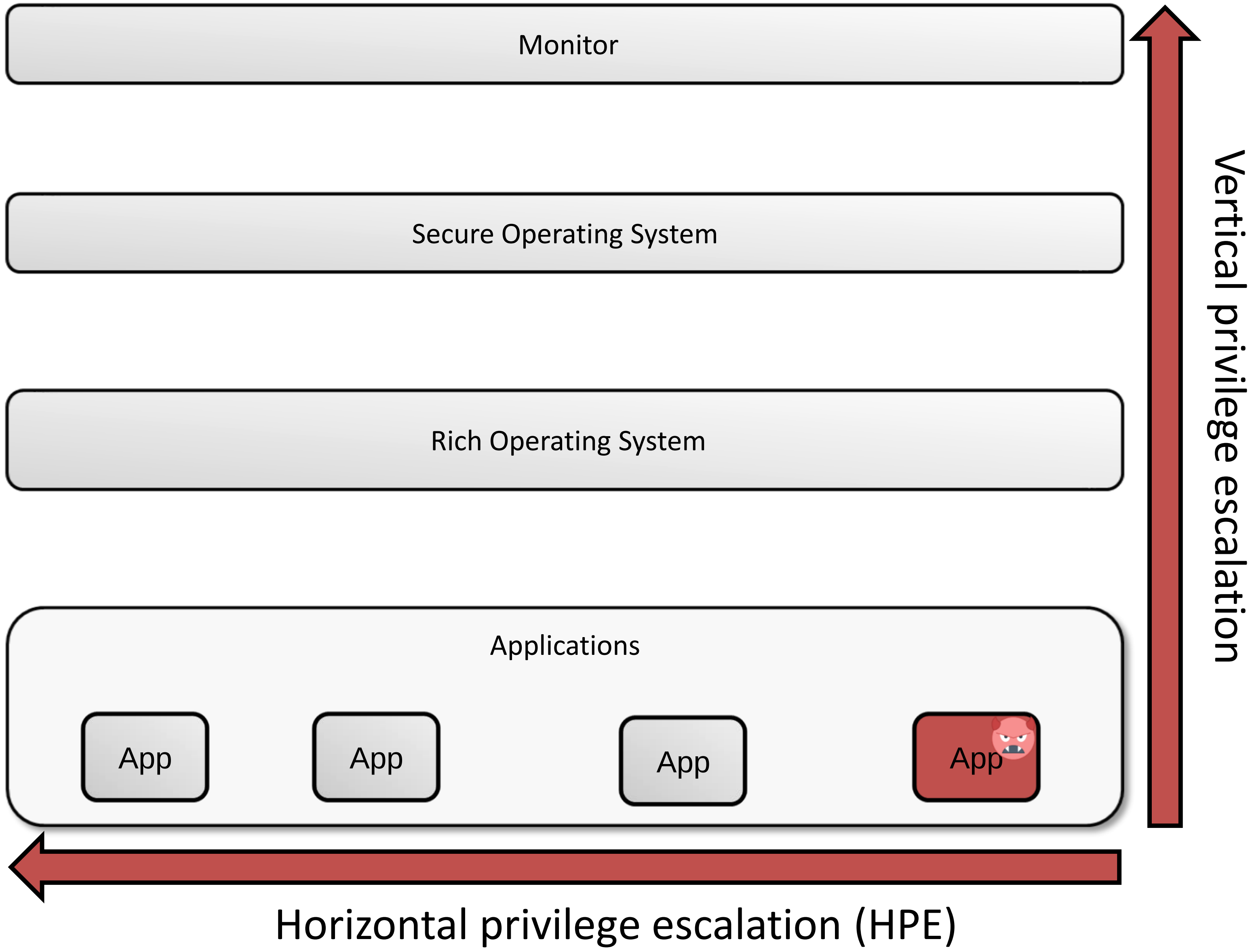


Background: Boomerang[1] attack

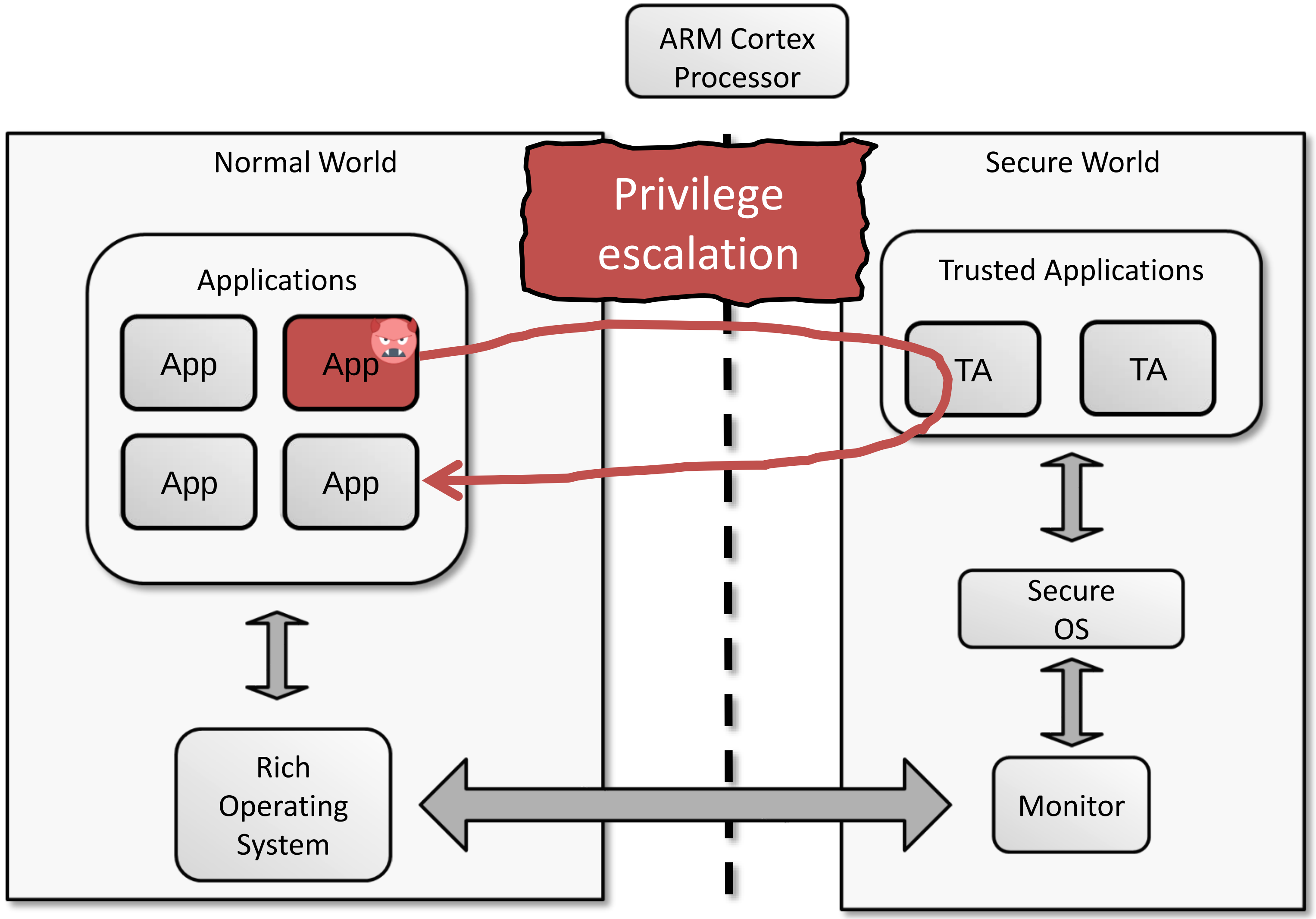


[1] Machiry, Aravind, et al. "BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments." *NDSS*. 2017.

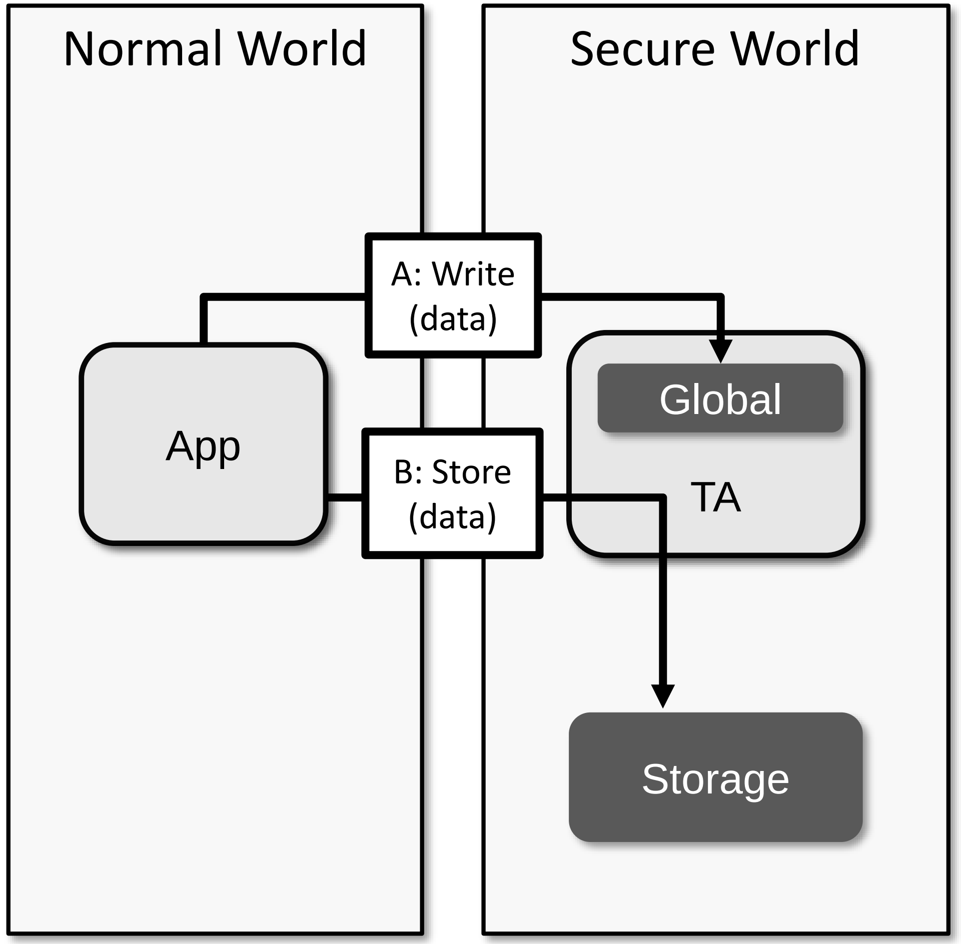
Background: Privilege escalation



HPE attack using TA

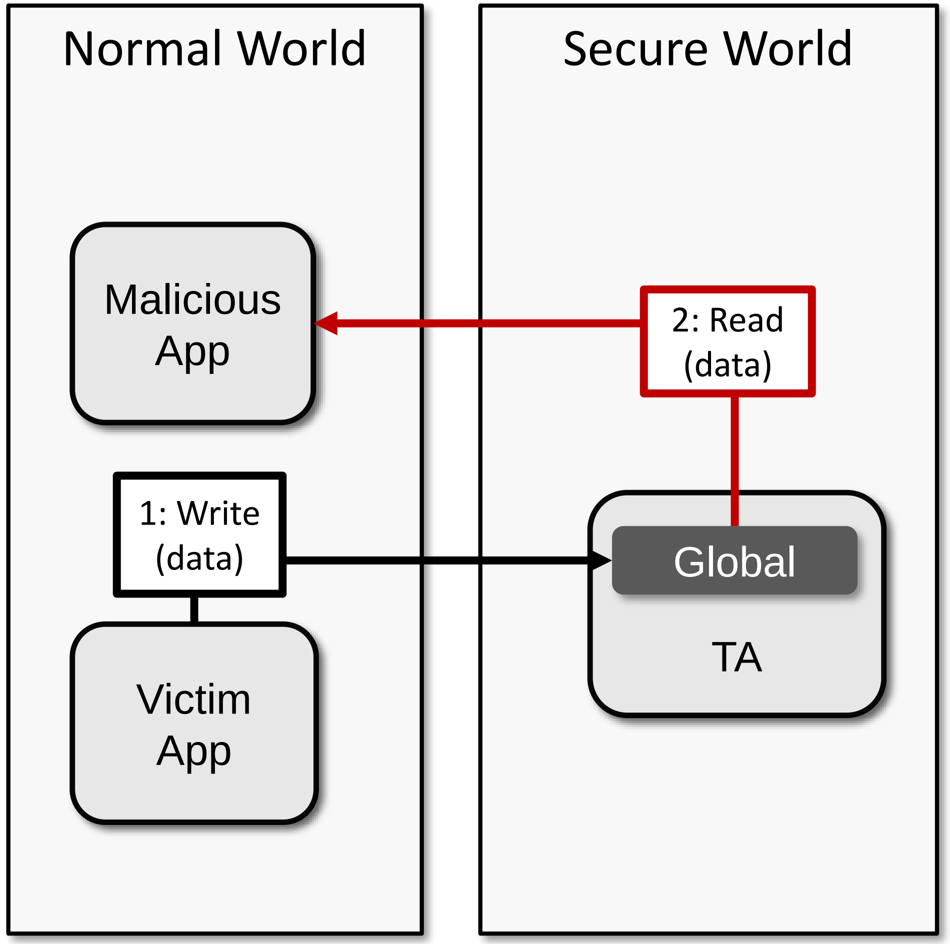


Storing data in Secure World

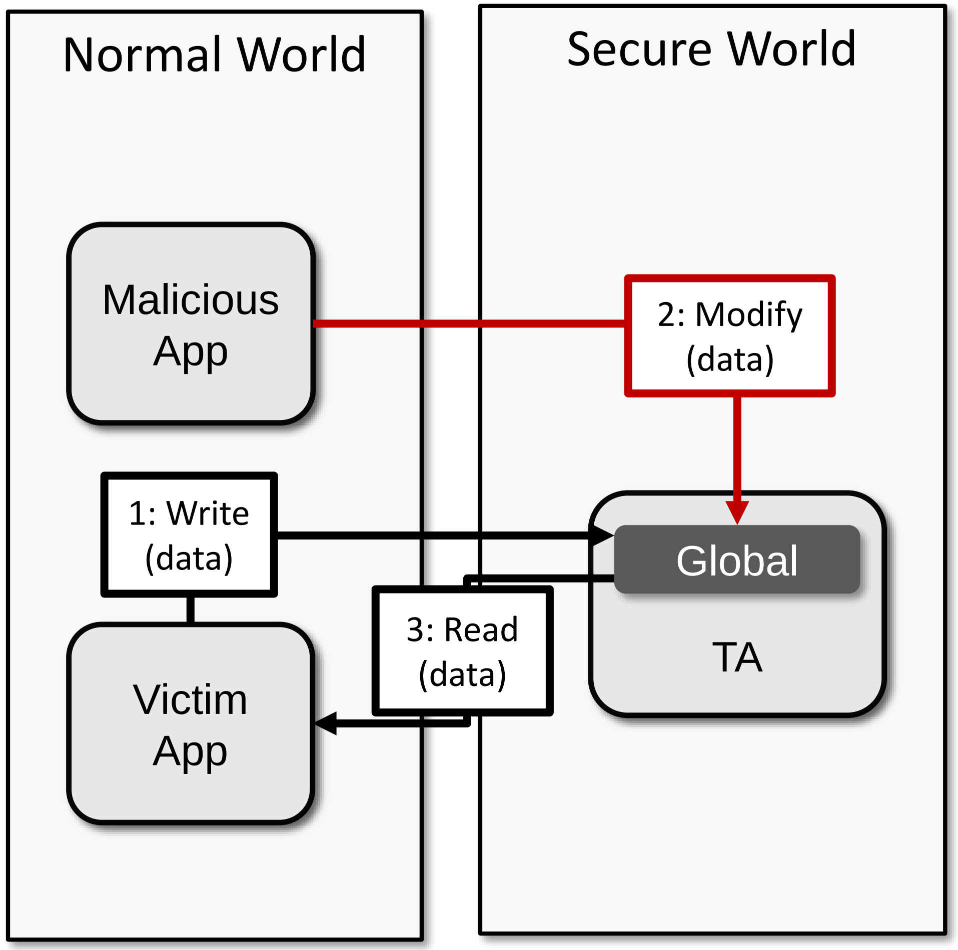


Global data attack examples

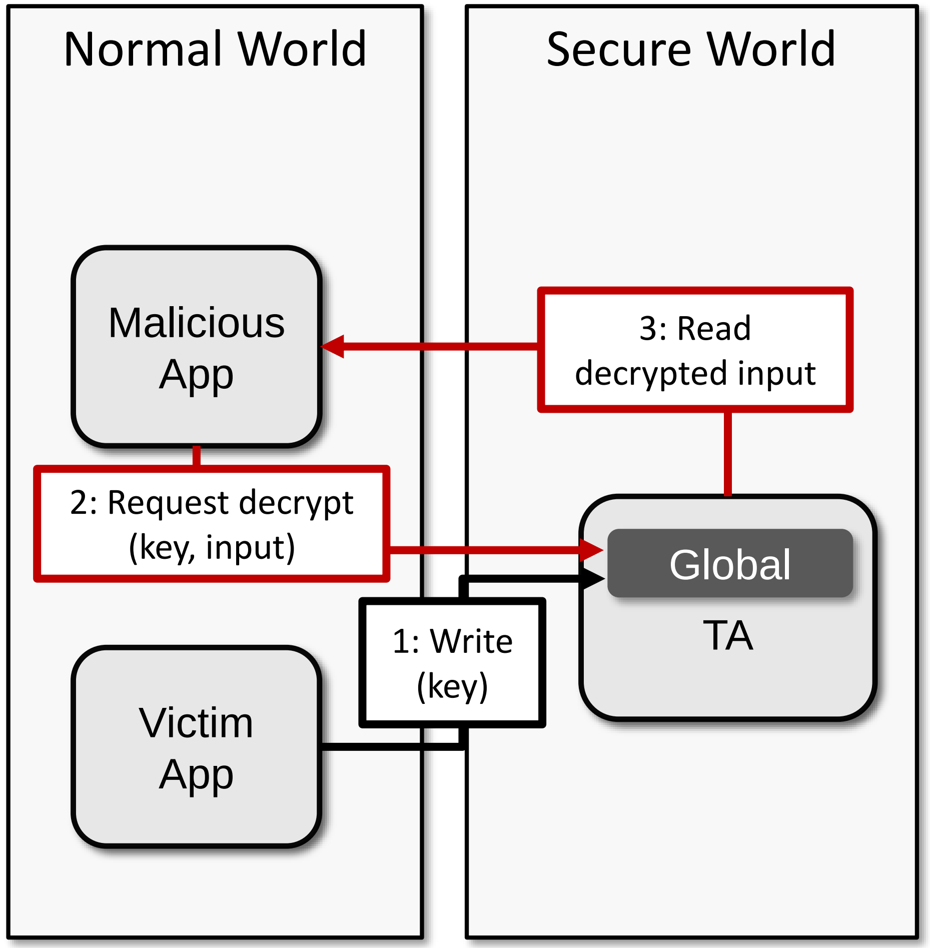
Data leakage



Data compromise

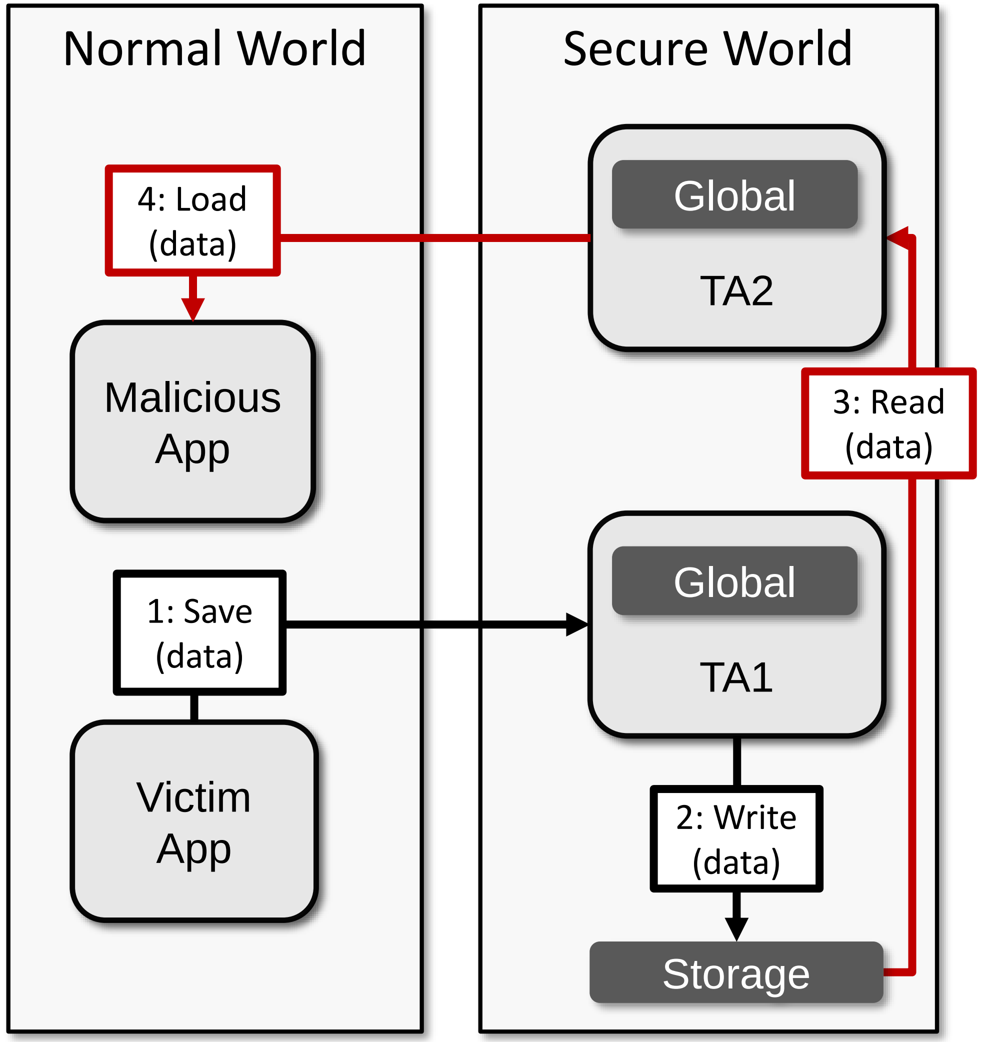


Decryption oracle

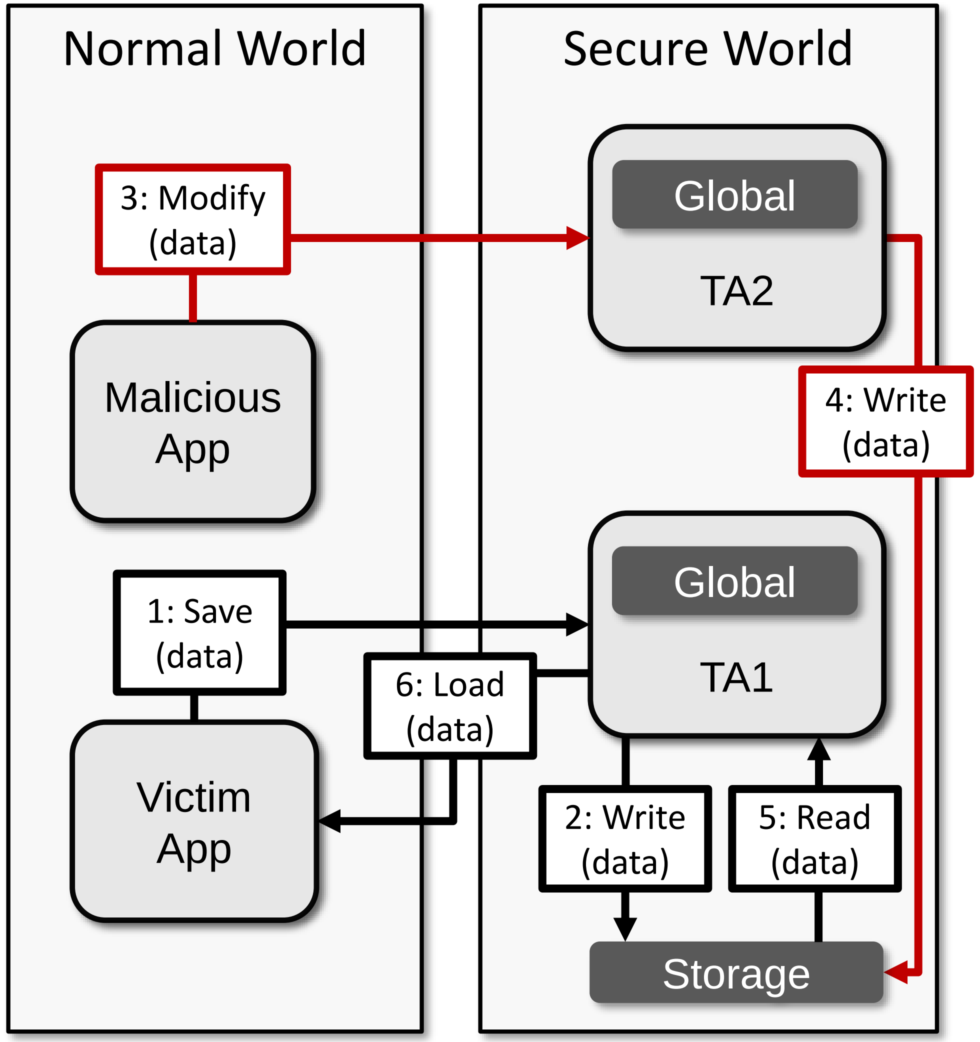


Stored data attack examples

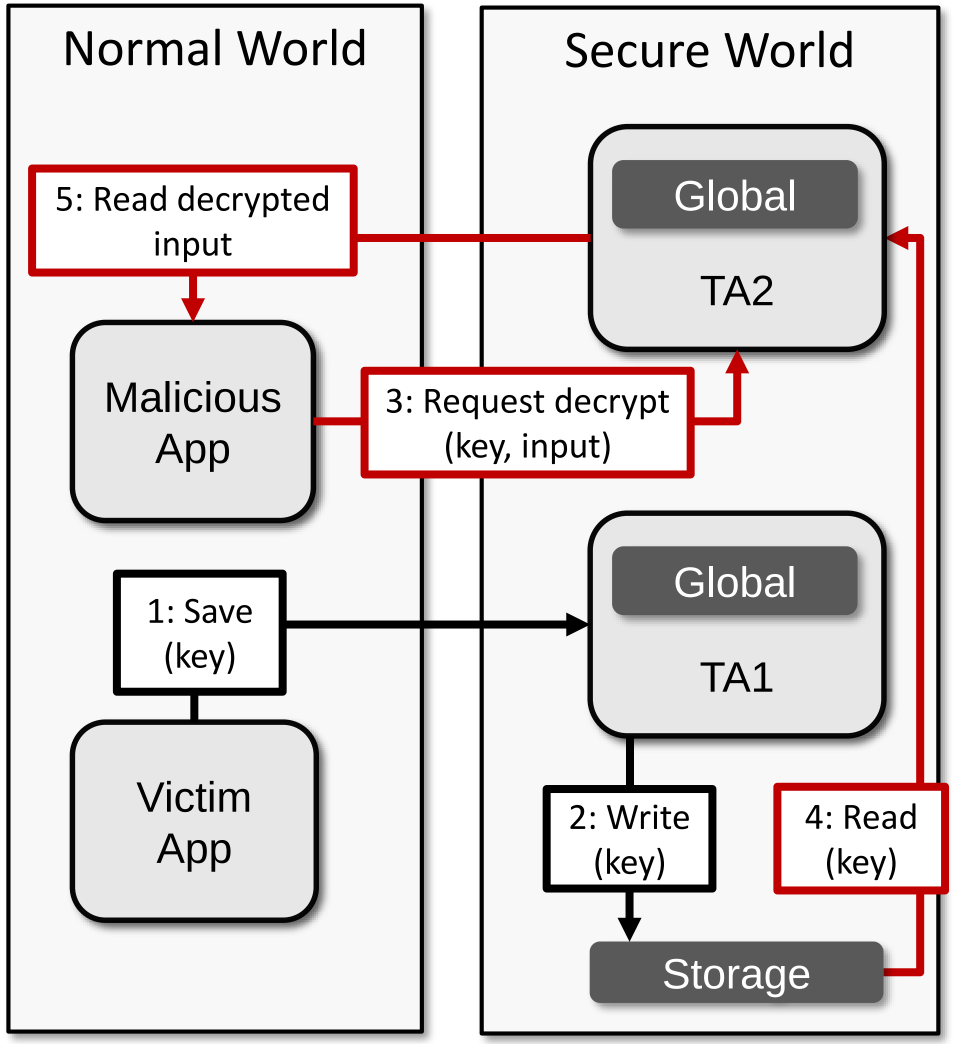
Data leakage



Data compromise



Decryption oracle



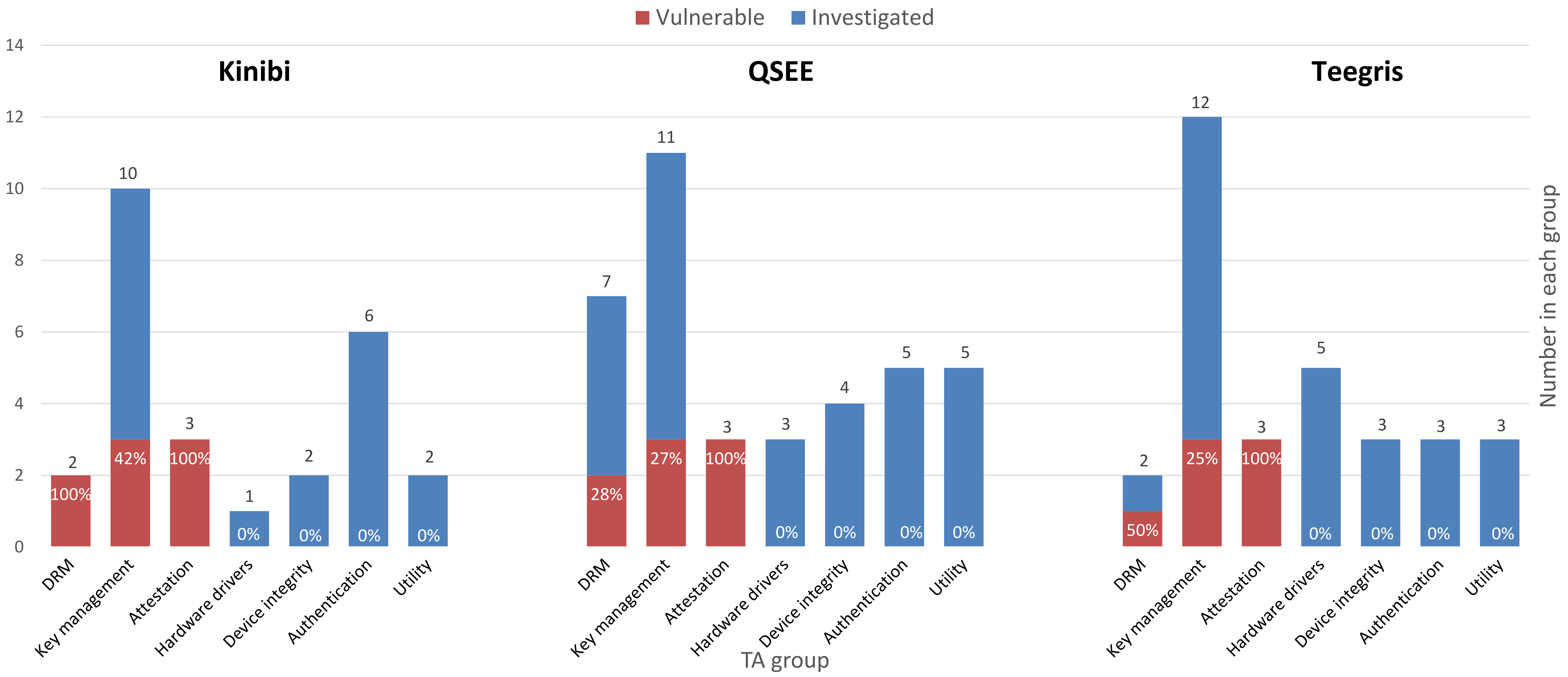
HPE manual analysis

95 TA binaries analyzed

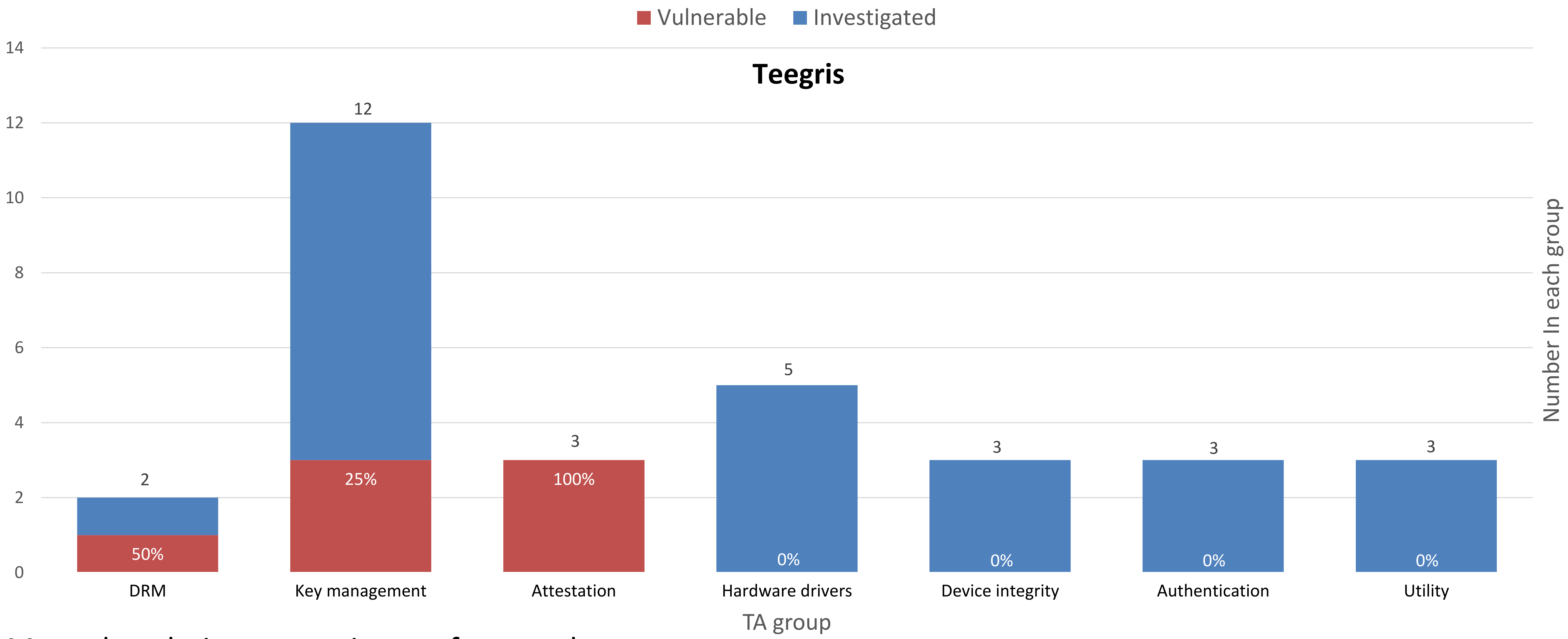
3 major TrustZone environments investigated (Kinibi, QSEE, Teegris)

HPE enabling vulnerabilities discovered (3 types)

Findings: vulnerable TAs



Findings: vulnerable TAs



Manual analysis: two engineers, four weeks

HPE vulnerability impact

Data leakage

Example: Encryption key leaked to attacker

Data compromise

Example: Encryption key replaced with attacker data

Decryption oracle

Example: DRM content decrypted for malicious app

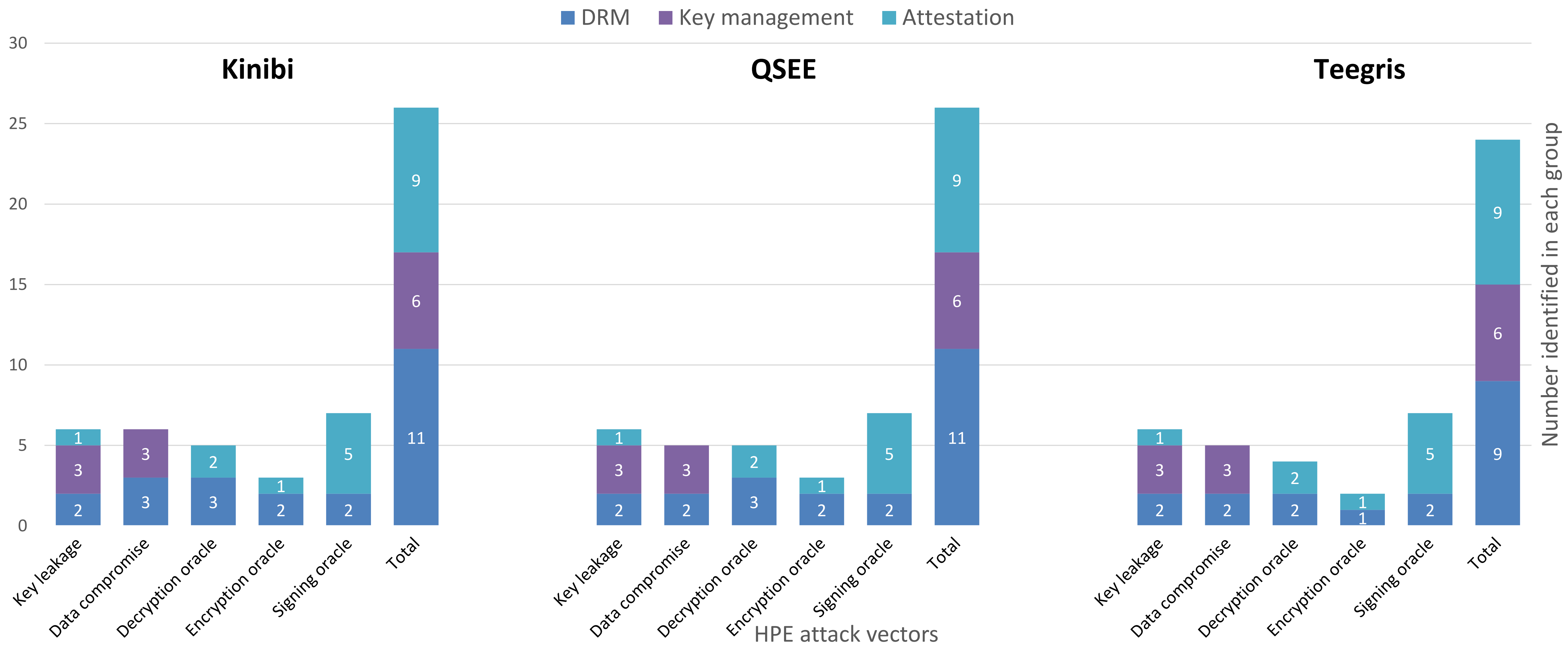
Encryption oracle

Example: Encrypted keys replaced with attacker data

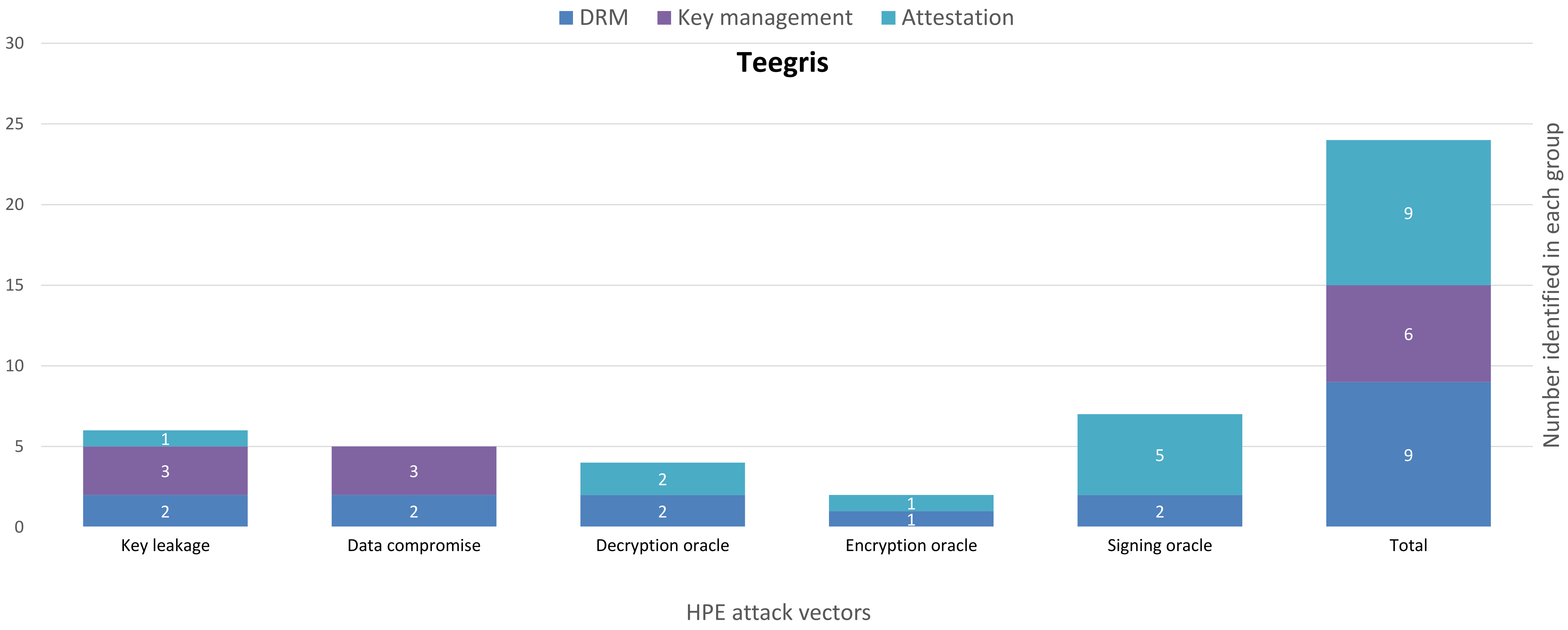
Signing oracle

Example: TA signs forged attestation data

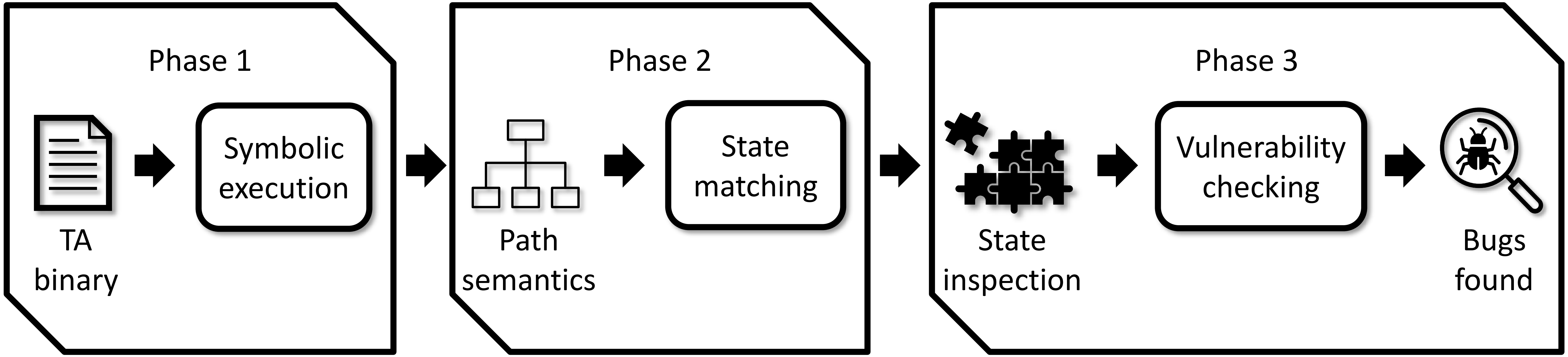
Findings: HPE attack vectors



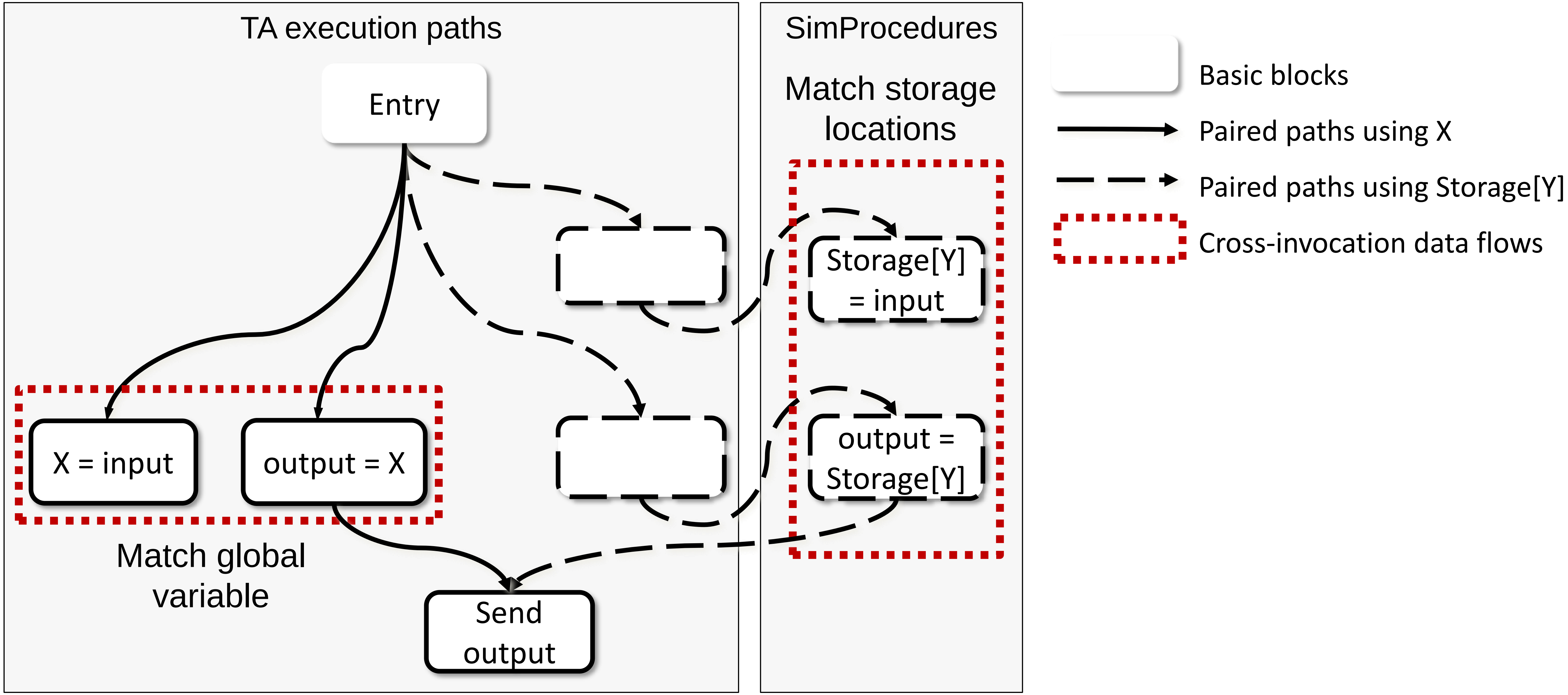
Findings: HPE attack vectors



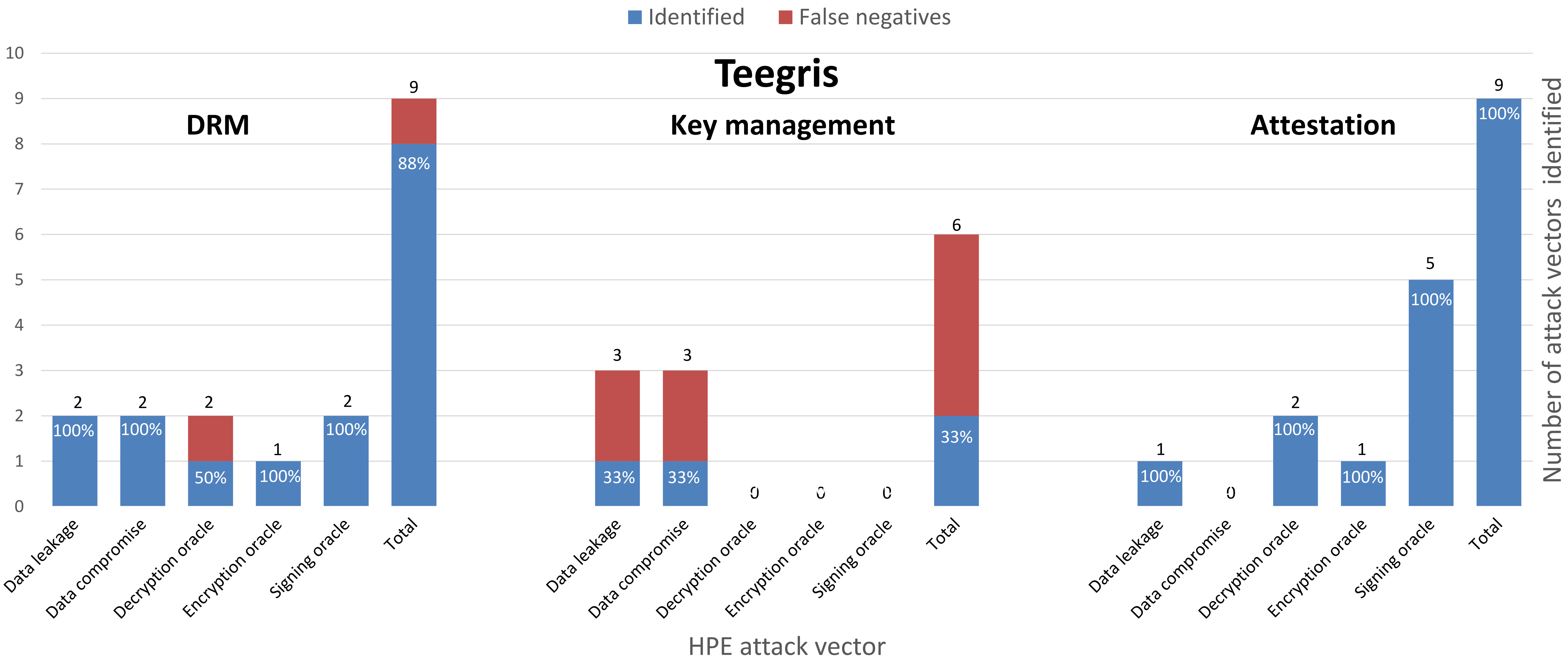
Hooper: Automatic HPE detection



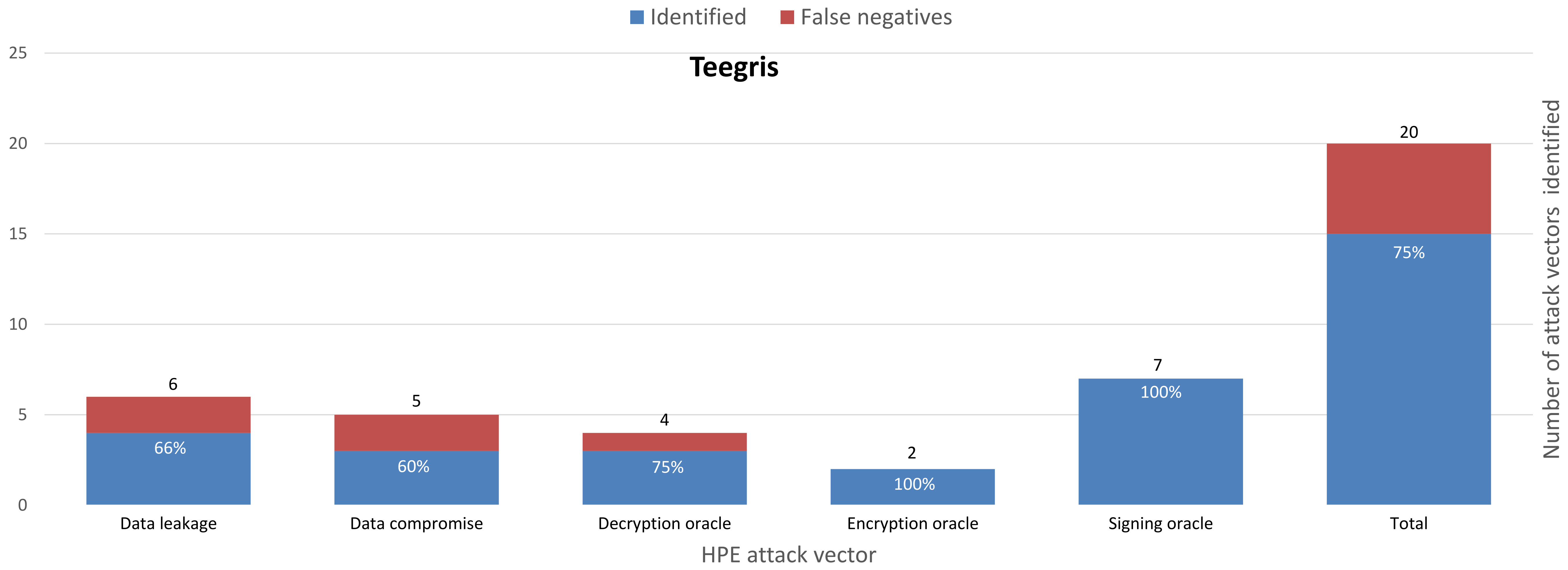
Hooper: Cross-invocation tracking



Automatic analysis results



Automatic analysis results



Vulnerabilities found in 24 hours vs 4 weeks of manual analysis

Mitigations

Resolve TA multi-tenant interference

Introduce session management inside all multi-tenant TAs

Standardized TA session management

Introduce a library for managing sessions inside TAs

Fine-grained access to Secure World storage

Partition Secure World storage and enforce fine-grained access control

Minimize access to TAs

Use fine-grained access policies to prevent unauthorized access to TAs

Conclusion

Some TAs store data from multiple applications across invocations

Insufficient access control exposes TA-managed data to attackers

Three type of HPE-enabling vulnerabilities found in 23 TAs

Automatic binary analysis can help identify HPE vulnerabilities

Platform-wide fine-grained access control would help mitigate HPE

Thank you!

Contact information:

Darius Suciu ➡ dsuciu@cs.stonybrook.edu

Stephen McLaughlin ➡ s.mclaughlin@samsung.com

Laurent Simon ➡ cam.lmrs2@gmail.com

Radu Sion ➡ sion@cs.stonybrook.edu

Questions?