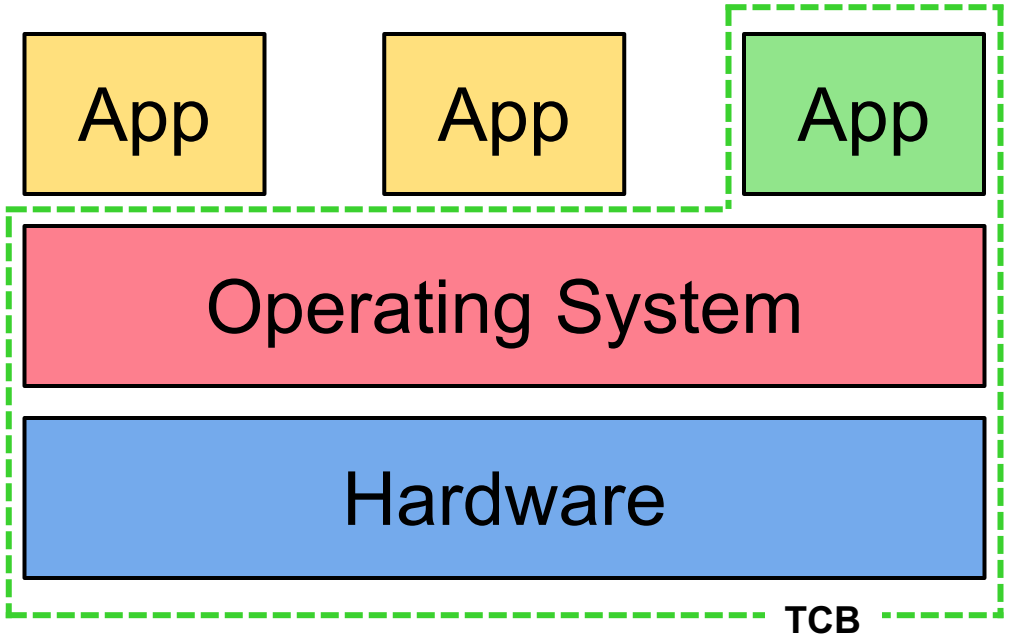
ETH zürich

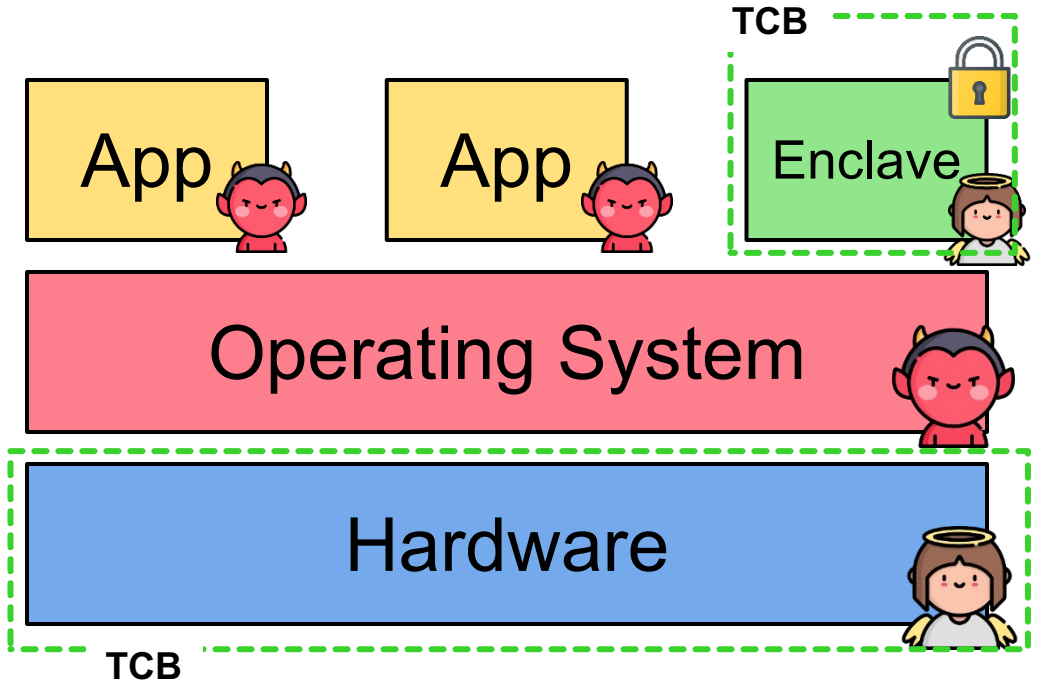
ProximiTEE: Hardened SGX Attestation using Auxiliary Device and Proximity Verification

Aritra Dhar, Ivan Puddu, Kari Kostiainen and Srdjan Capkun
ETH Zurich

Motivation: Intel SGX

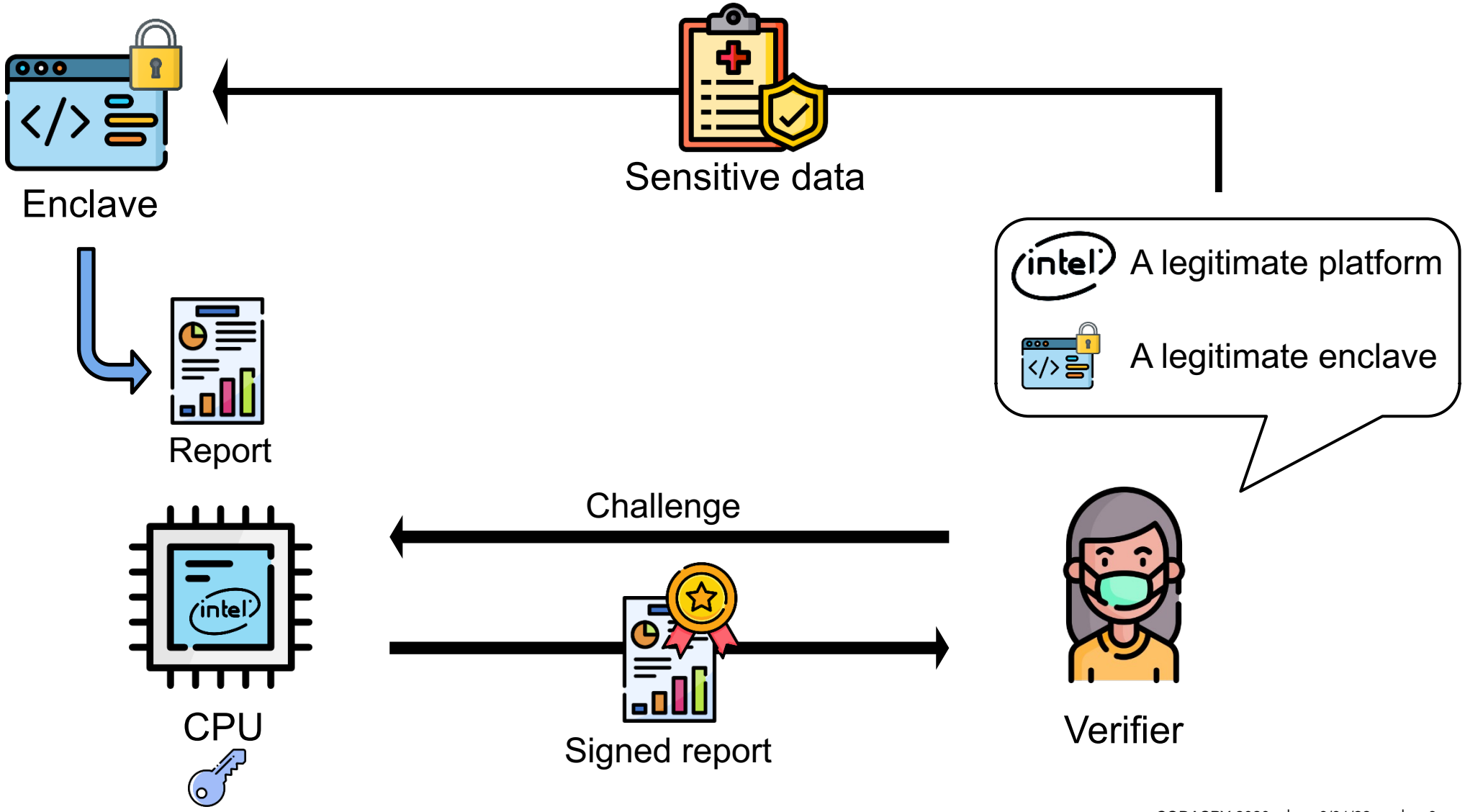


Traditional platforms

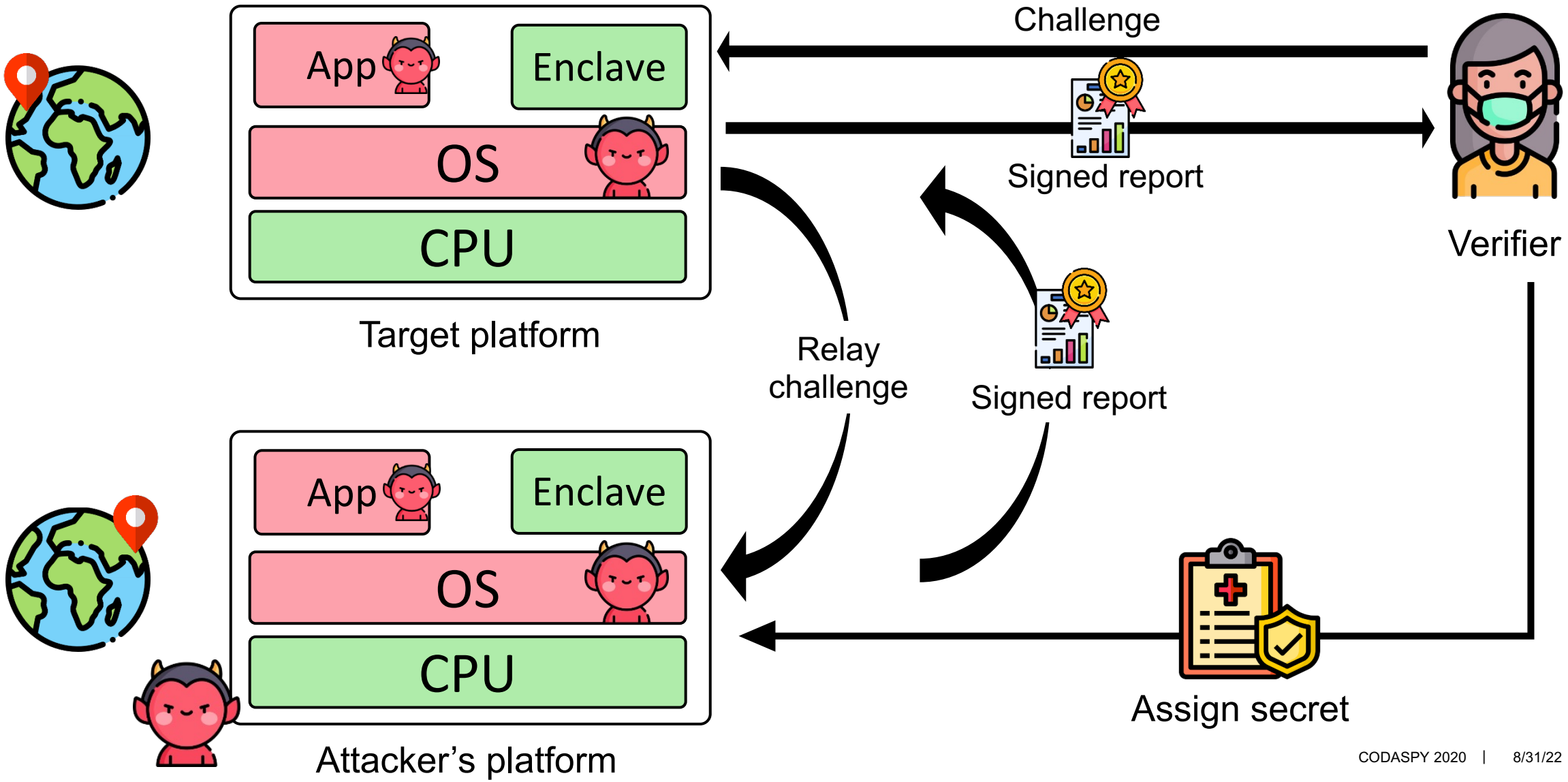


Intel SGX

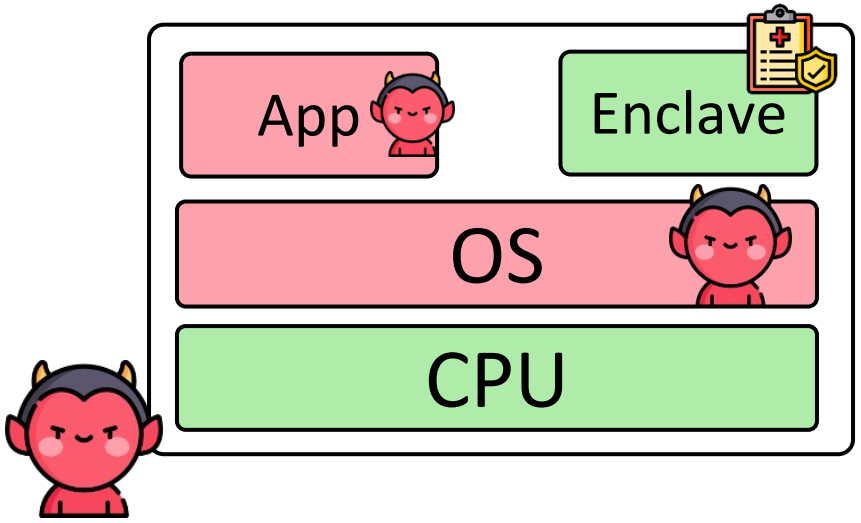
Motivation: Remote Attestation



Common issue: Relay Attacker

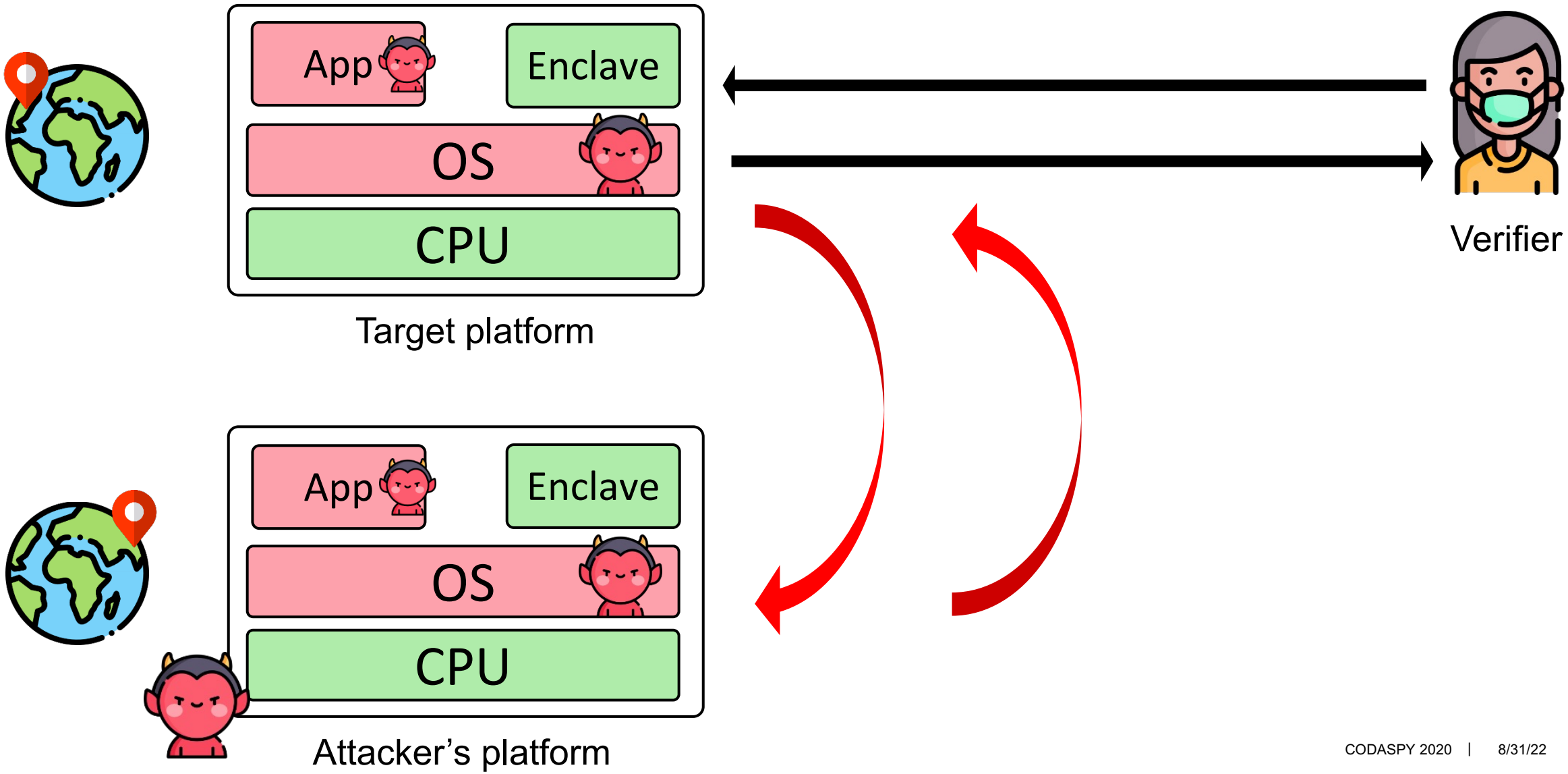


Our Contribution: Relay Attack Implications

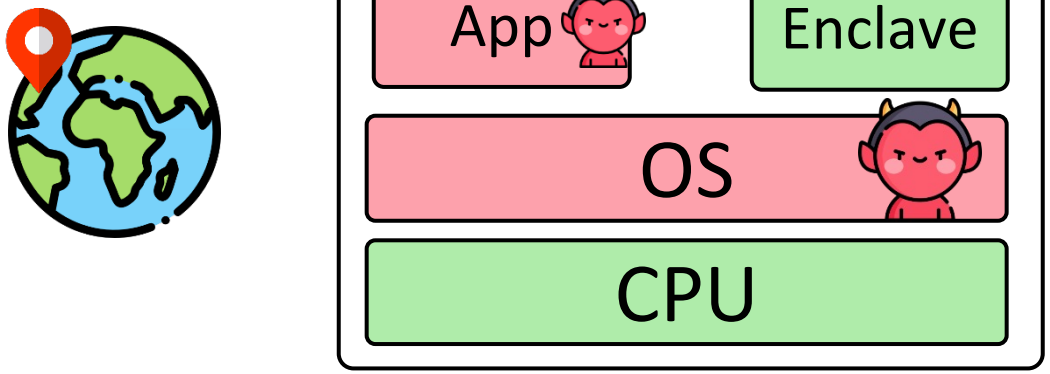


- Physical access
- Privilege escalation
- Undermine platform maintenance
  - Defer patch
  - Secure target platform
  - Insecure attacker's platform

Distinguishing is hard



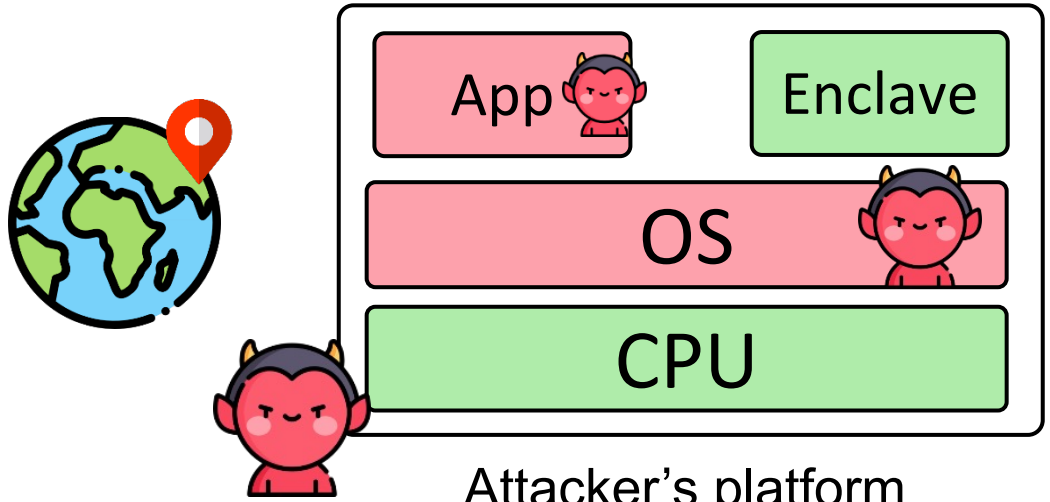
Our Contribution: Auxiliary Device



Target platform

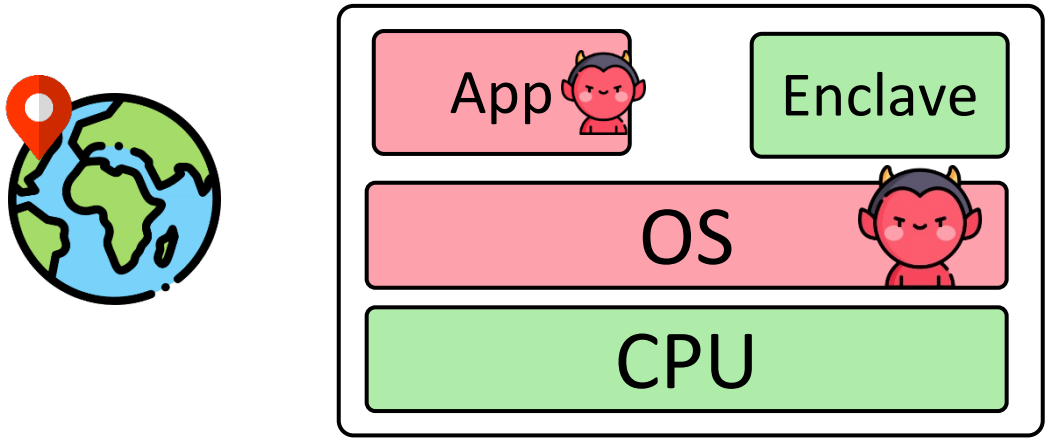
ProximiKey

Verifier

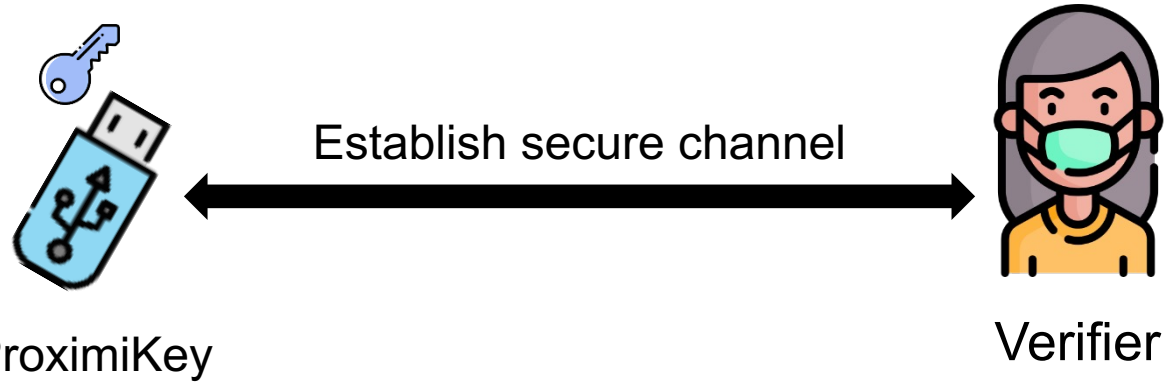


Attacker's platform

ProximiTEE

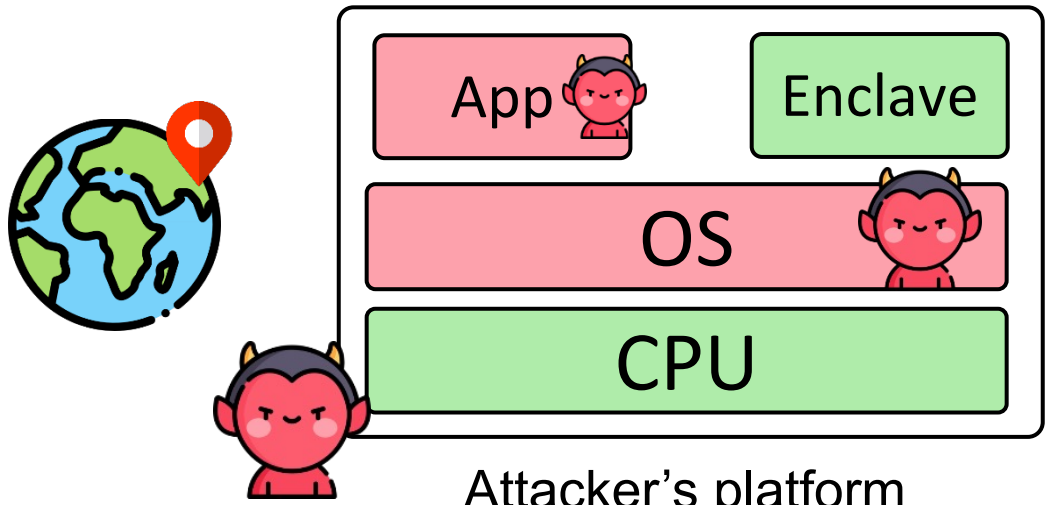


Target platform



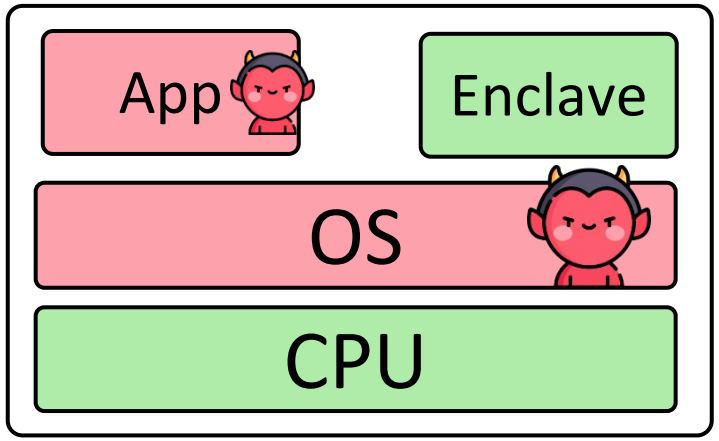
ProximiKey

Verifier



Attacker's platform

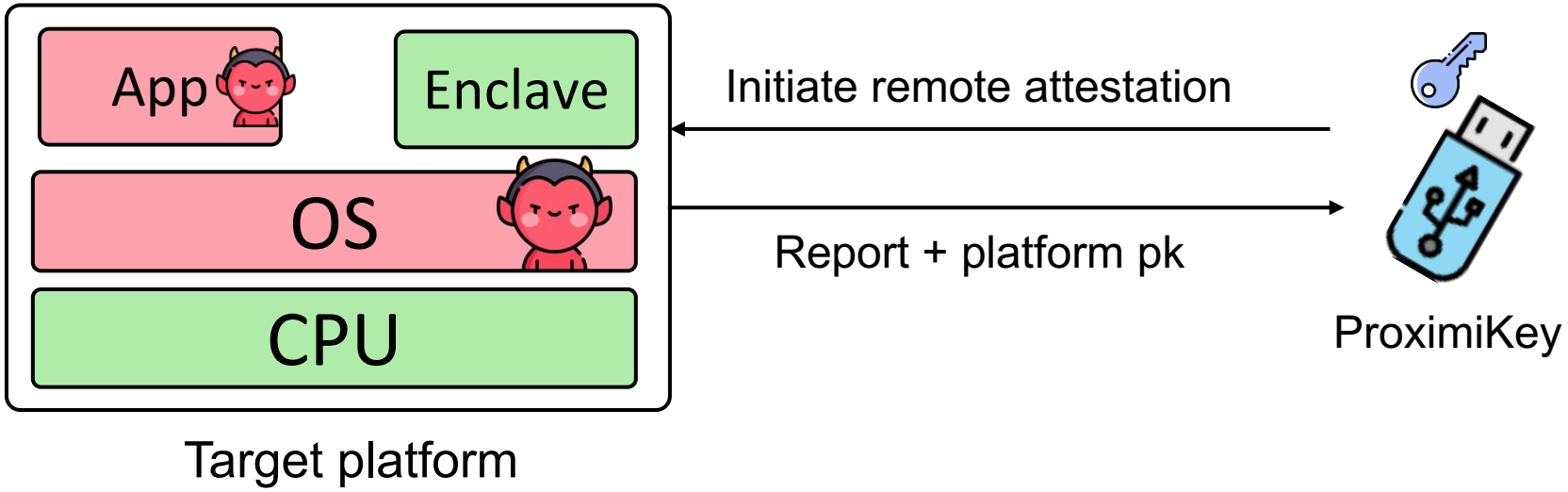
ProximiTEE



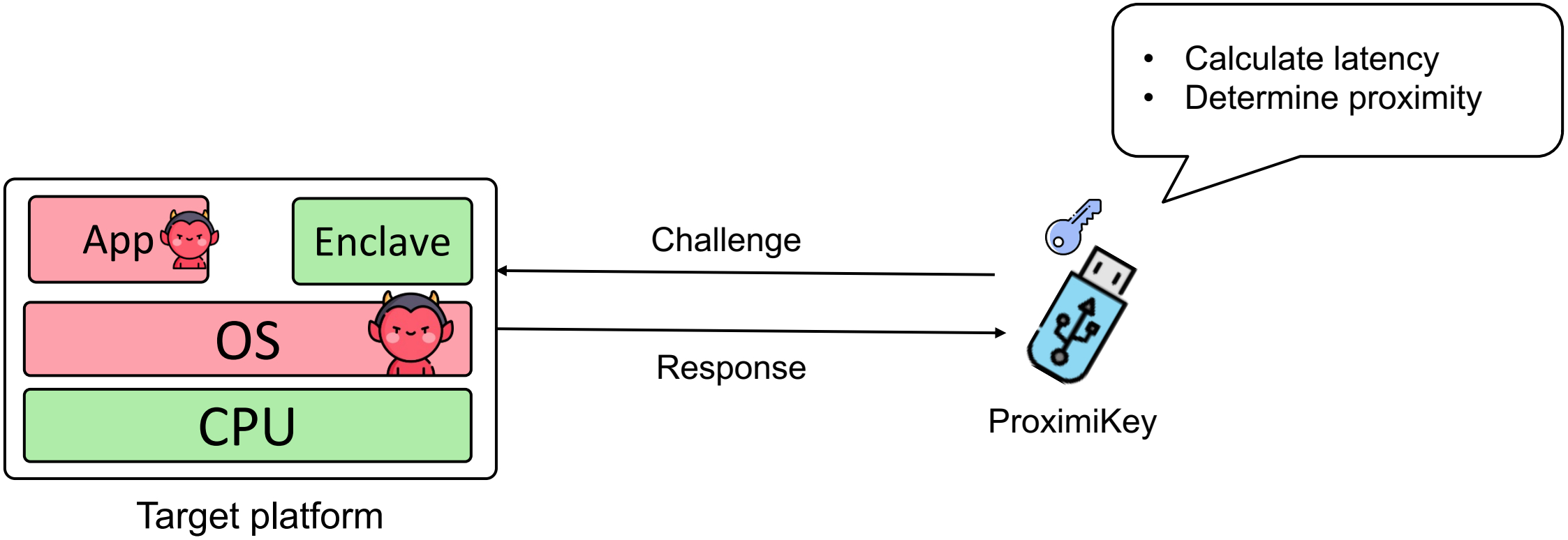
Target platform

ProximiKey

ProximiTEE

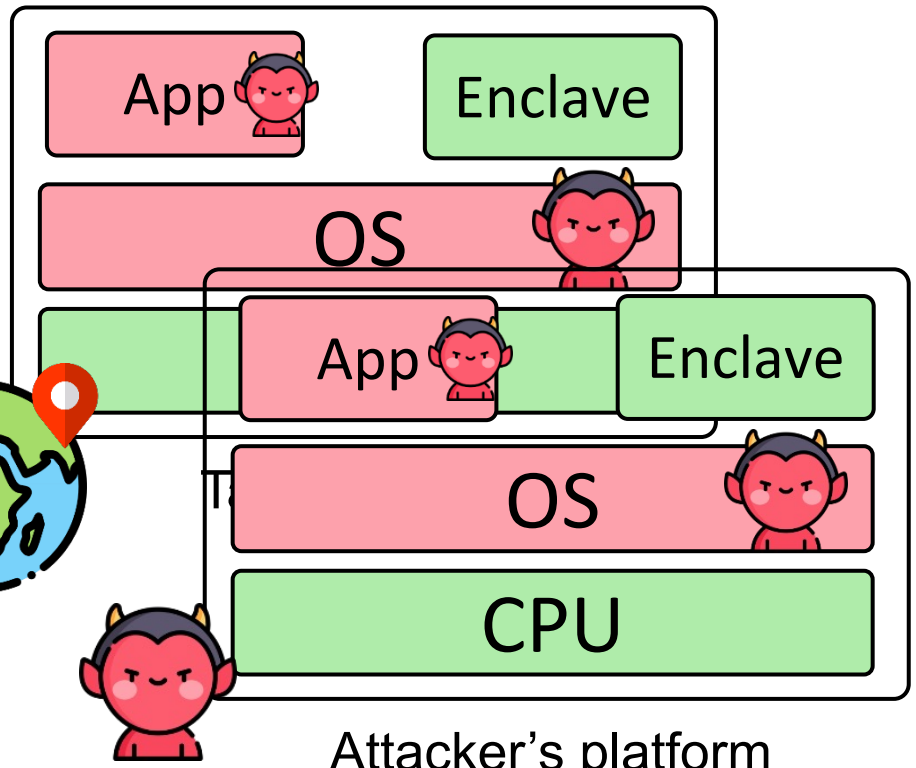

App
Enclave
OS
CPU
Target platform
Initiate remote attestation
Report + platform pk
ProximiKey

ProximiTEE


• Calculate latency
• Determine proximity
App
Enclave
OS
CPU
Target platform
Challenge
Response
ProximiKey

ProximiTEE

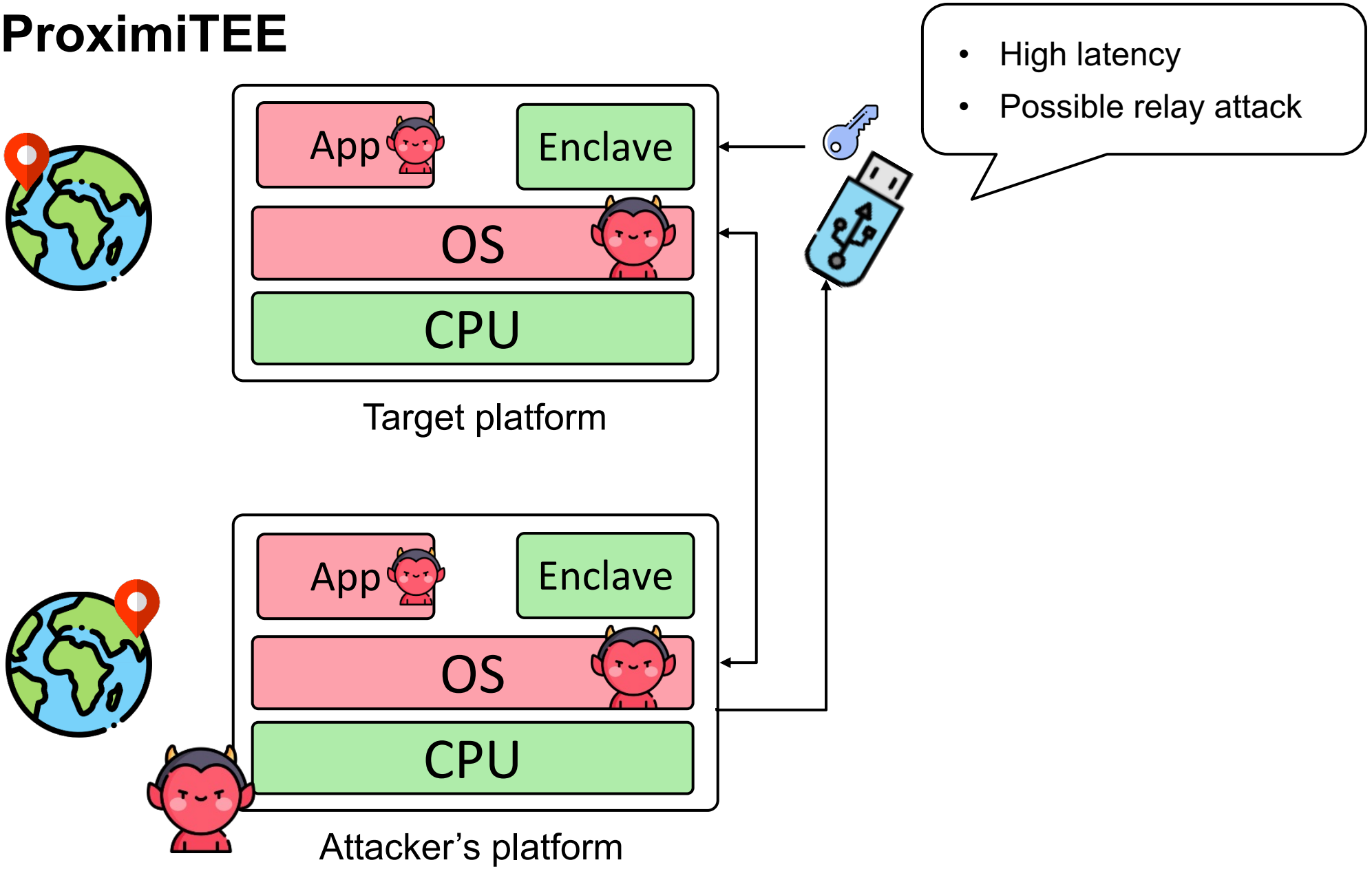
Verifier



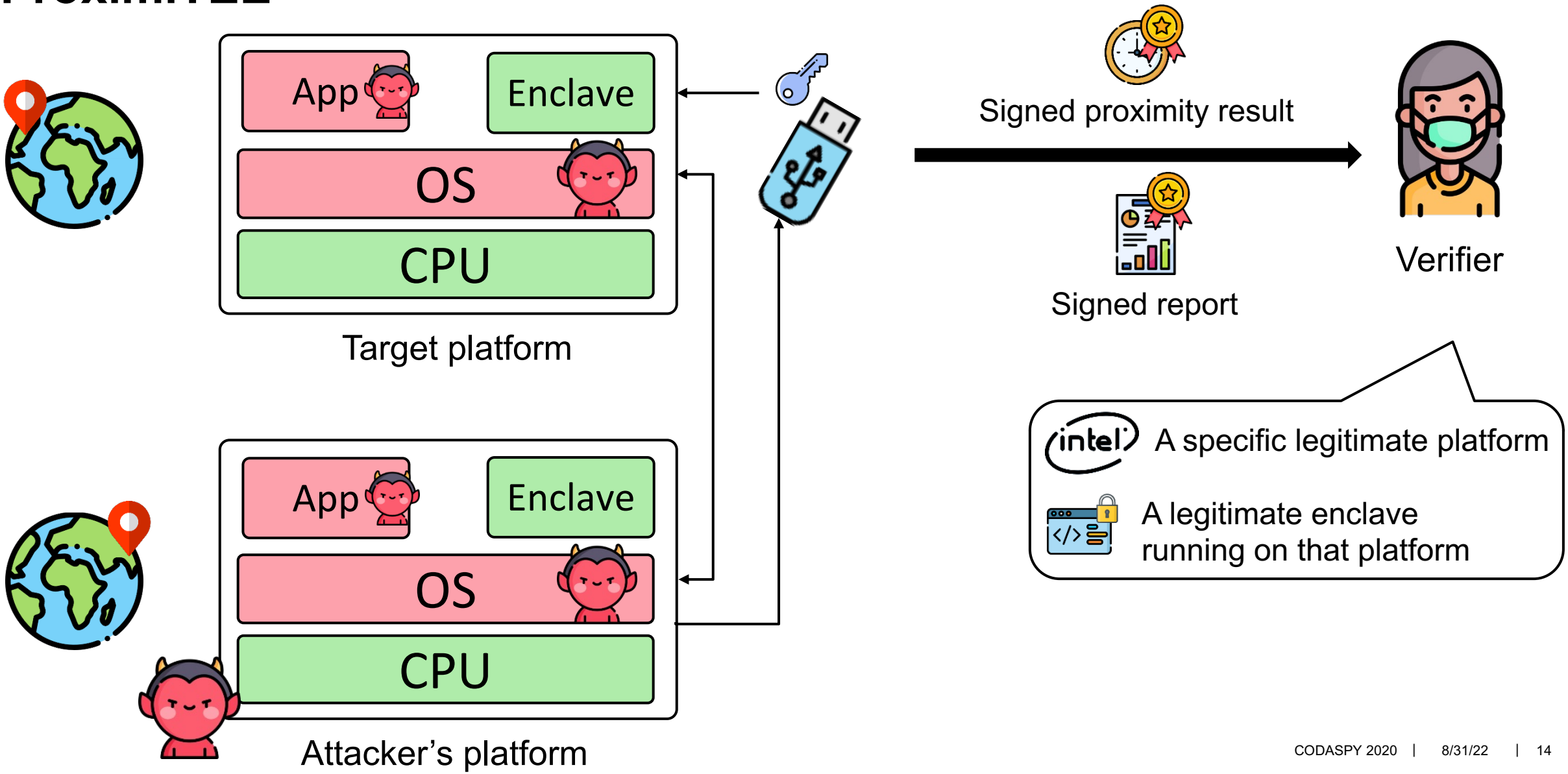
Attacker's platform

ProximiKey

ProximiTEE

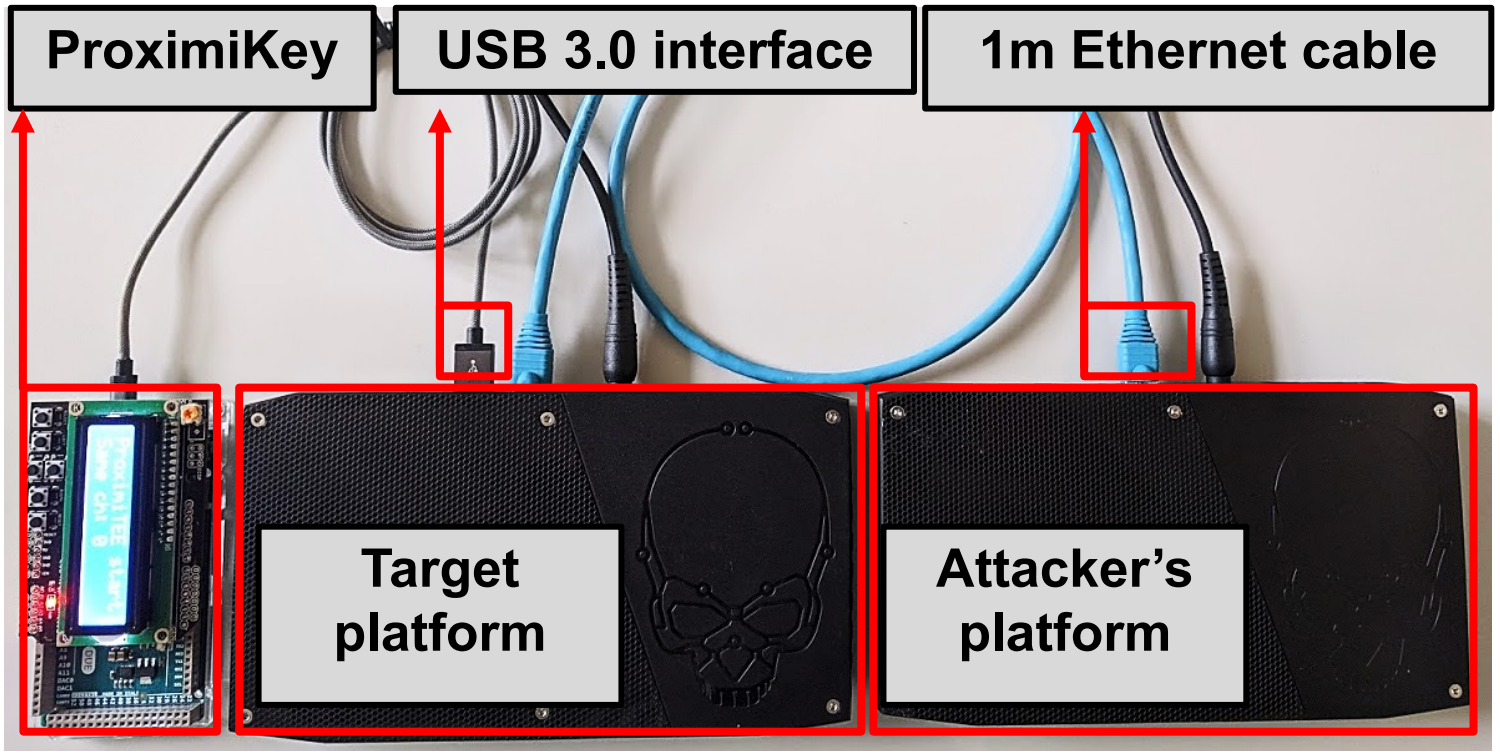

App
Enclave
OS
CPU
Target platform
App
Enclave
OS
CPU
Attacker's platform
• High latency
• Possible relay attack
Verifier

ProximiTEE

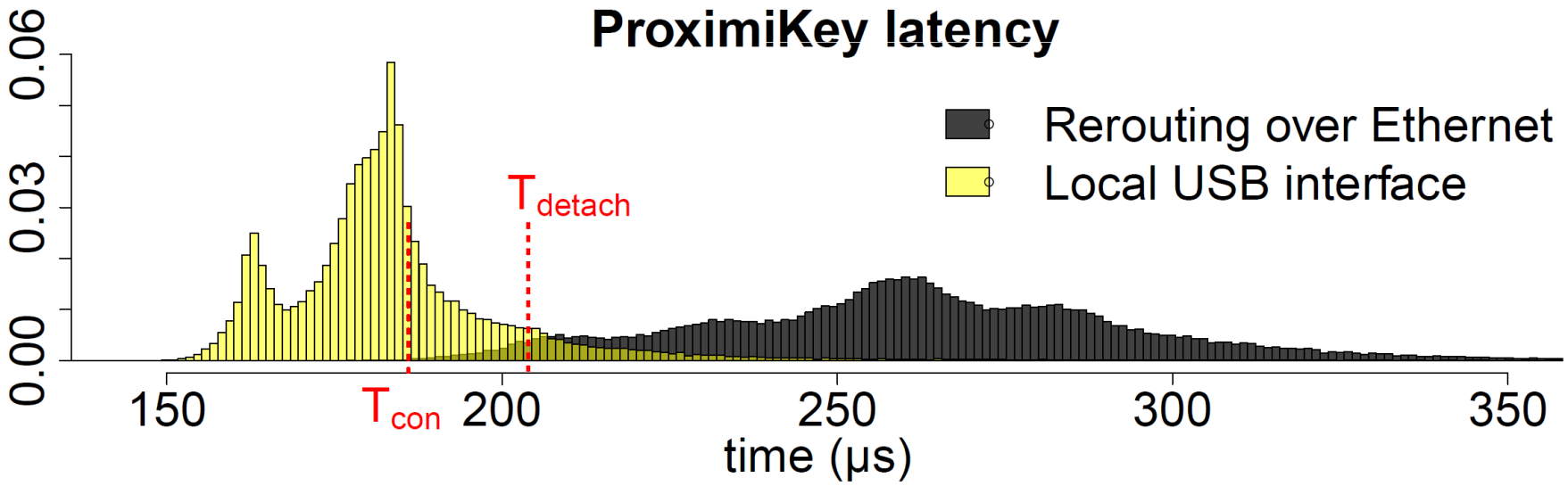

App
Enclave
OS
CPU
Target platform
App
Enclave
OS
CPU
Attacker's platform
Signed proximity result
Signed report
Verifier
intel
A specific legitimate platform
A legitimate enclave
running on that platform

Evaluation: Setup

- Fully implemented
  - ProximiKey based on **Cypress EZ-USB FX3**
  - ProximiTEE API
- **Simulated** powerful attacker
  - 1-meter Ethernet connection
  - Instant computation
  - Zero-latency NIC
- Ping flood mode
  - $RTT = 158\,\mu s$

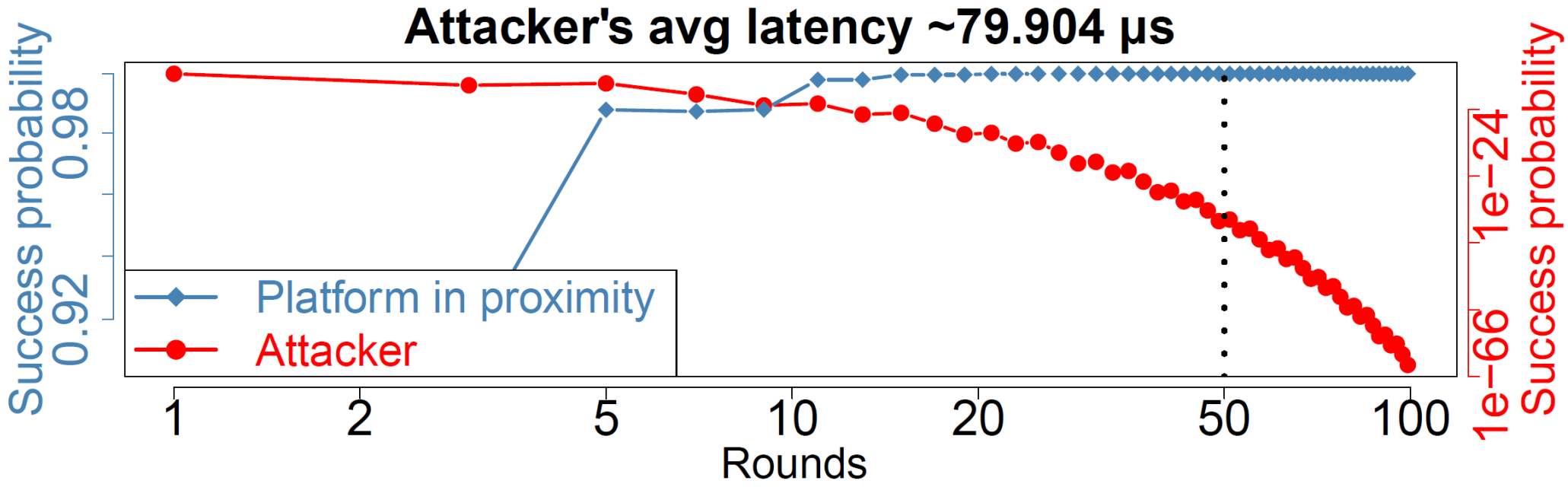


Main Experimental Result



- Local USB: Spans: $145 - 250\mu s$, average: $185\mu s$
- Ethernet: Spans: $200 - 750\mu s$, average: $264\mu s$
- Samples ($27.8M$ normal traces and $15M$ simulated attack traces)
- Multiple rounds

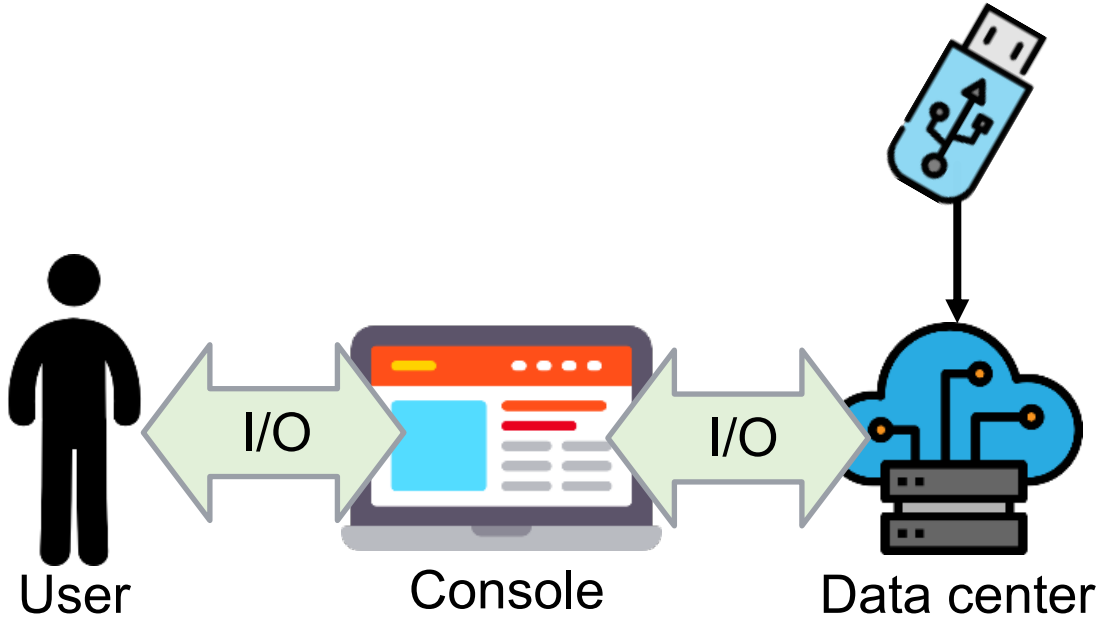
Proximity Verification Result



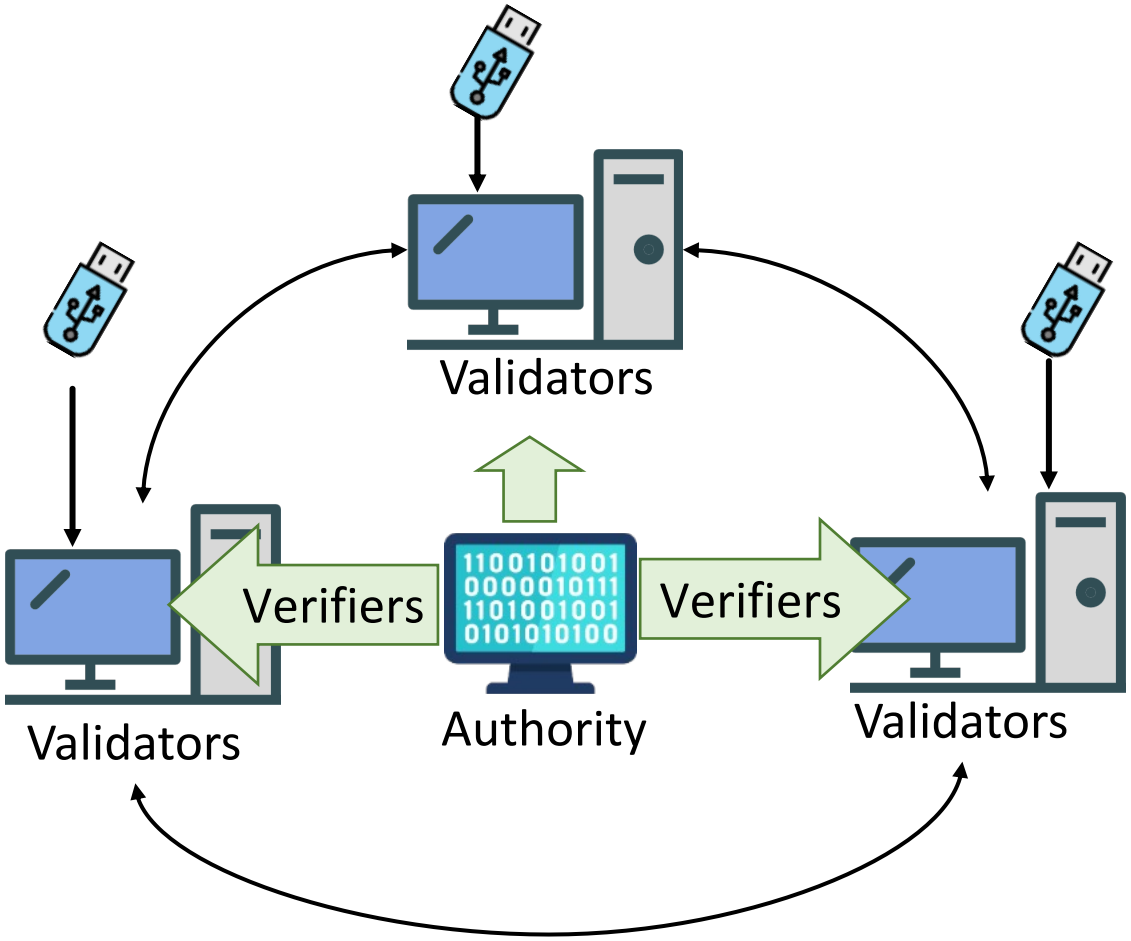
Robust: $P_{legit} = 0.999999977$

Secure: $P_{adv} = 3.55 \times 10^{-34}$ for 40 rounds

Potential Use case: Attestation of Enclave in Data Centre



Potential Use case: Setup of Permissioned Blockchain



Conclusion

- Intel SGX remote attestation
- Relay attack, implications and analysis
- ProximiTEE- leverages distance bounding and trusted embedded device
- Robust against the relay attacker and practical

Thank you! Questions?