barkhauseninstitut.org

barkhausen institut

Towards Modular Trusted Execution Environments

Carsten Weinhold[1], Nils Asmussen[1], Diana Göhringer[2], Michael Roitzsch[1]

[1]Barkhausen Institut
[2]Technische Universität Dresden

barkhausen institut

Towards Modular Trusted Execution Environments

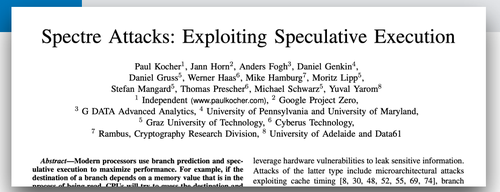
Part 1

Transport Layer Security + Remote Attestation

Part 2

Lots of TEEs, but not so much choice …

	TEE ISA	Implementation	TEE Type	Integration
Intel SGX	x86-64	complex core	enclave	libOS / wrapper
Intel TDX	x86-64	complex core	VM	standalone
AMD SVM	x86-64	complex core + PSP	VM	standalone
Arm CCA	Armv9	complex core	VM	standalone
Sanctum	RISC-V	core + mitigation	enclave	libOS / wrapper
Sancus	TI MSP430	simple core	enclave / module	???


Spectre Attacks: Exploiting Speculative Execution

Paul Kocher[1], Jann Horn[2], Anders Fogh[3], Daniel Genkin[4], Daniel Gruss[5], Werner Haas[6], Mike Hamburg[7], Moritz Lipp[5], Stefan Mangard[5], Thomas Prescher[6], Michael Schwarz[5], Yuval Yarom[8]
[1] Independent (www.paulkocher.com), [2] Google Project Zero, [3] G DATA Advanced Analytics, [4] University of Pennsylvania and University of Maryland, [5] Graz University of Technology, [6] Cyberus Technology, [7] Rambus, Cryptography Research Division, [8] University of Adelaide and Data61


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

Jo Van Bulck[1], Marina Minkin[2], Ofir Weisse[3], Daniel Genkin[3], Baris Kasikci[3], Frank Piessens[1], Mark Silberstein[2], Thomas F. Wenisch[3], Yuval Yarom[4], and Raoul Strackx[1]
[1]*imec-DistriNet, KU Leuven,* [2]*Technion,* [3]*University of Michigan,* [4]*University of Adelaide and Data61*


2019 IEEE Symposium on Security and Privacy

RIDL: Rogue In-Flight Data Load

Stephan van Schaik*, Alyssa Milburn*, Sebastian Österlund*, Pietro Frigo*, Giorgi Maisuradze†‡, Kaveh Razavi*, Herbert Bos*, and Cristiano Giuffrida*
*Department of Computer Science, Vrije Universiteit Amsterdam, The Netherlands
†CISPA Helmholtz Center for Information Security, Saarland Informatics Campus

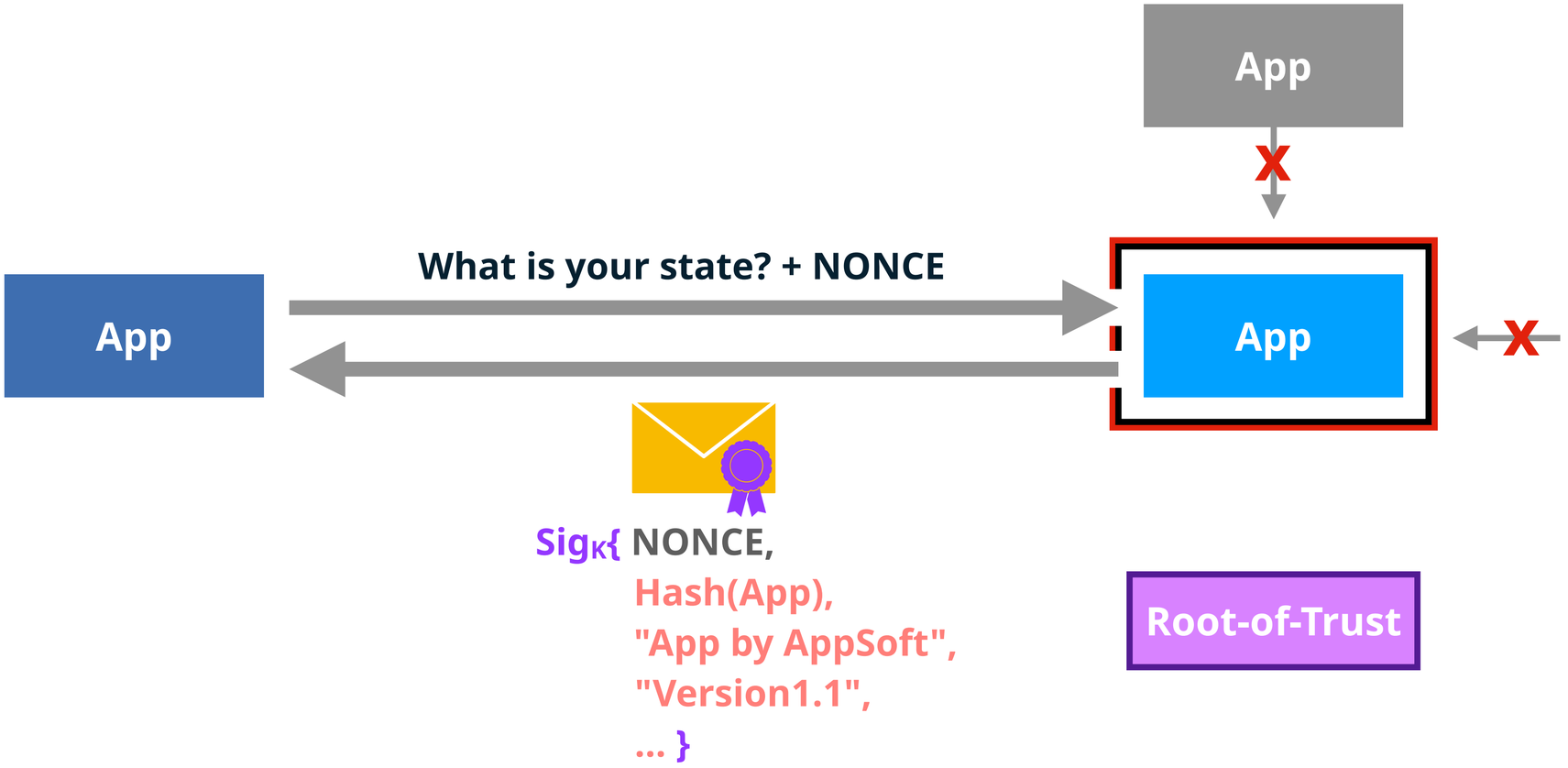
Problems with Current TEE Implementations

- TEE and ISA cannot be chosen independently
- TEE implementation deeply integrated in core microarchitecture
- TEEs lack "good" integration with system software

barkhausen
institut

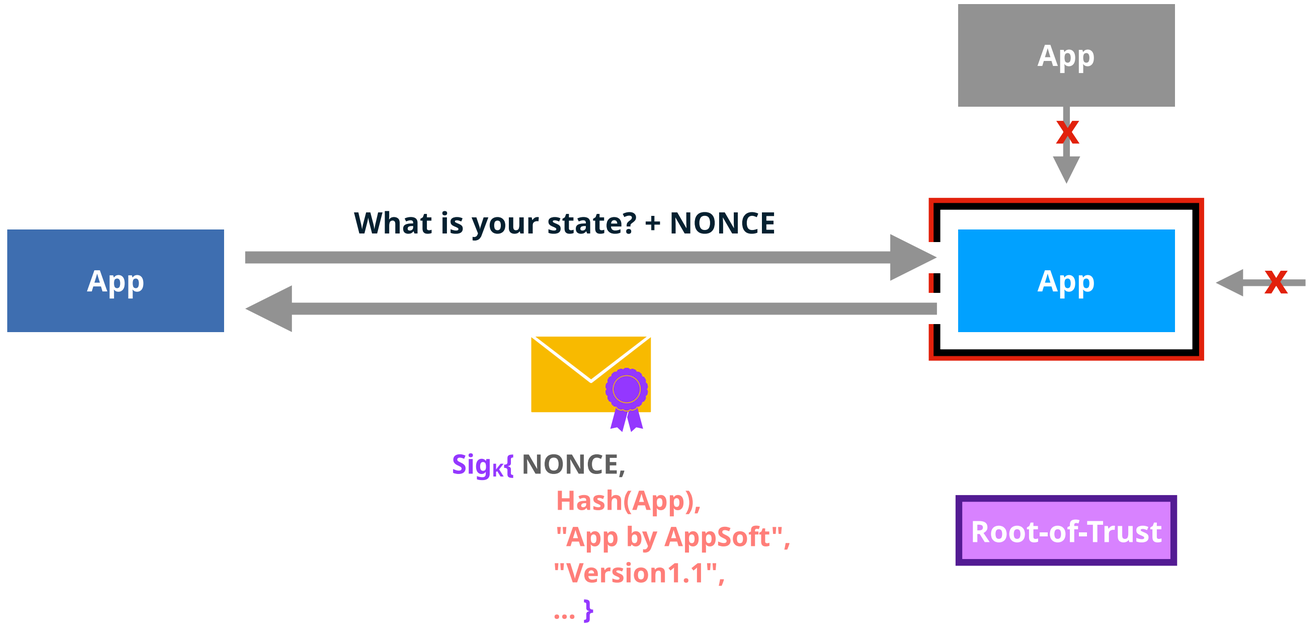
The Case for Modular TEEs

What is a Trusted Execution Environment?

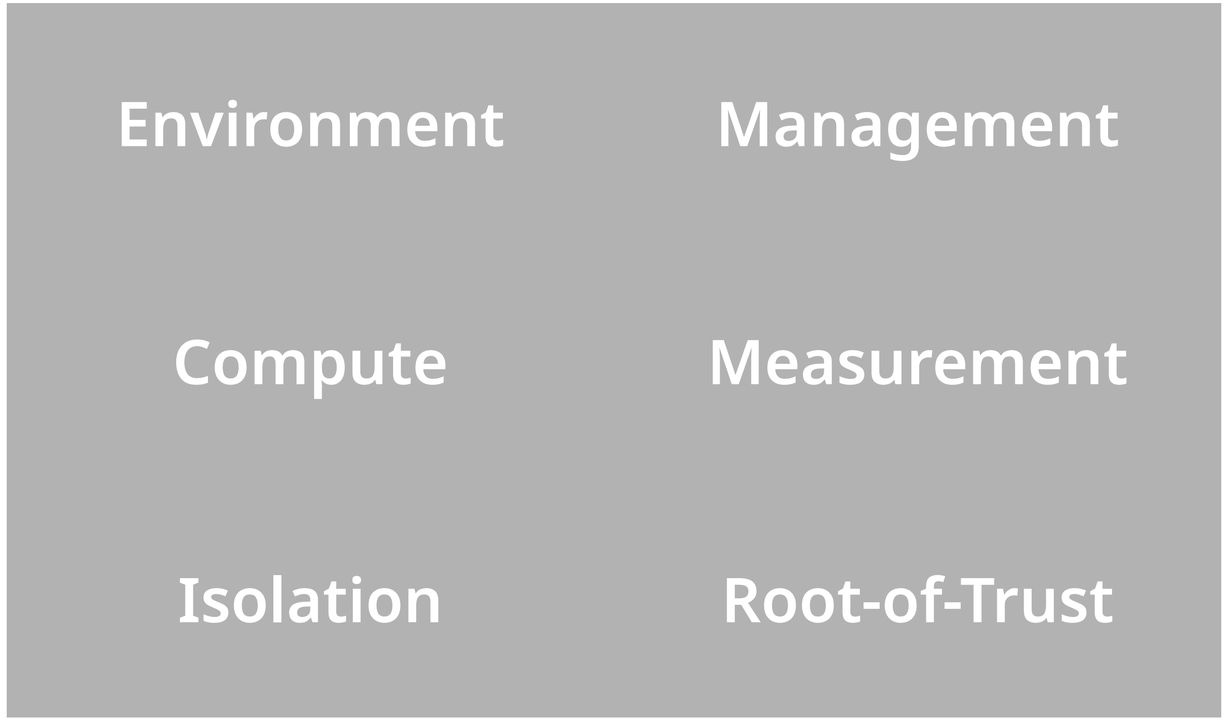


Six Concerns for TEE Design and Implementation

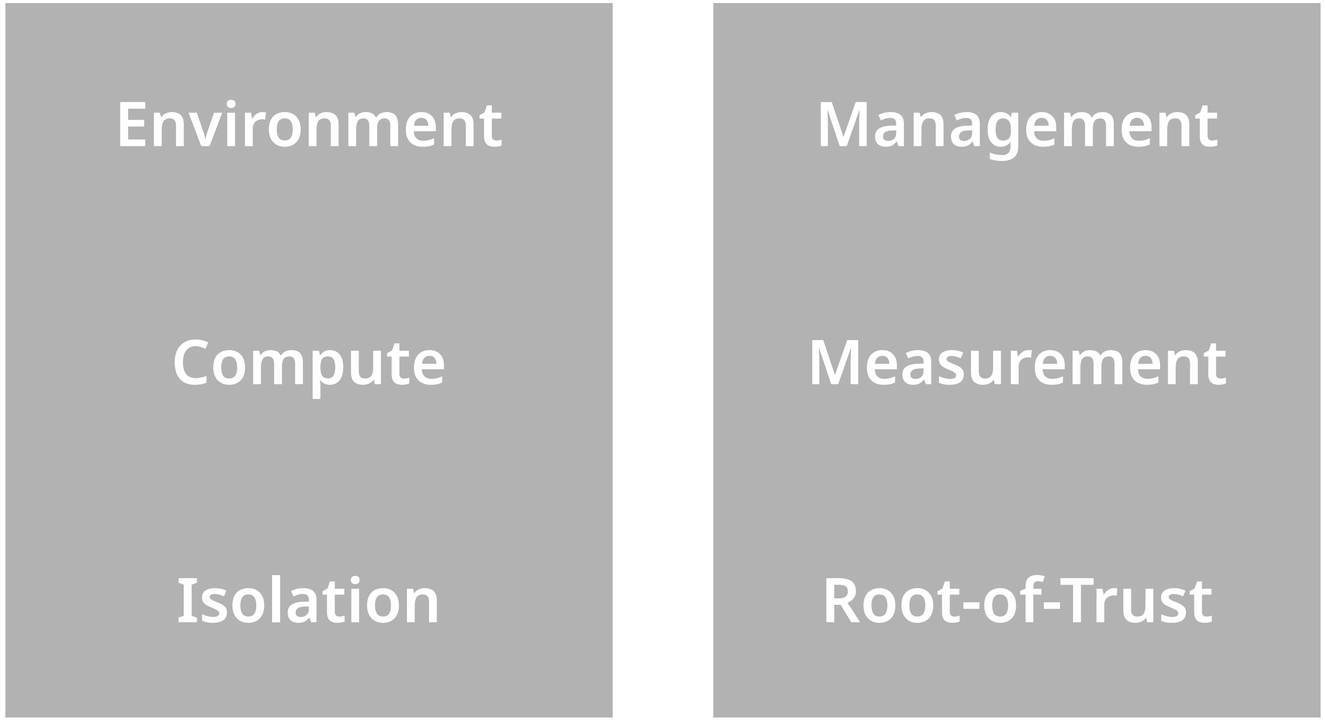
- Computation
- Measurement
- Root of Trust
- Isolation
- Management
- Environment



Breaking up TEE Design and Implementation



Breaking up TEE Design and Implementation



Breaking up TEE Design and Implementation

Environment

Management

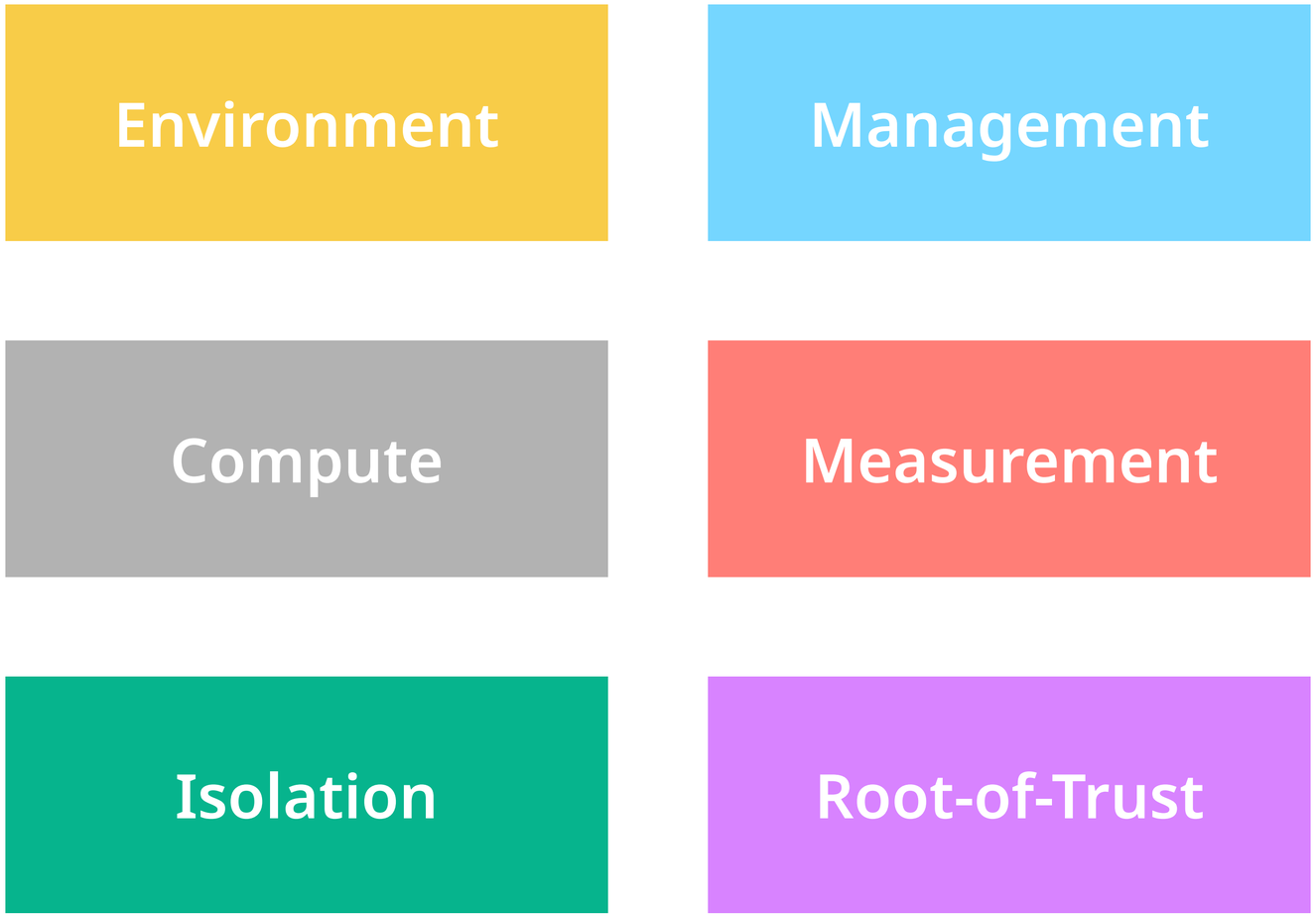
Compute

Measurement

Isolation

Root-of-Trust

Modularize TEE Design and Implementation



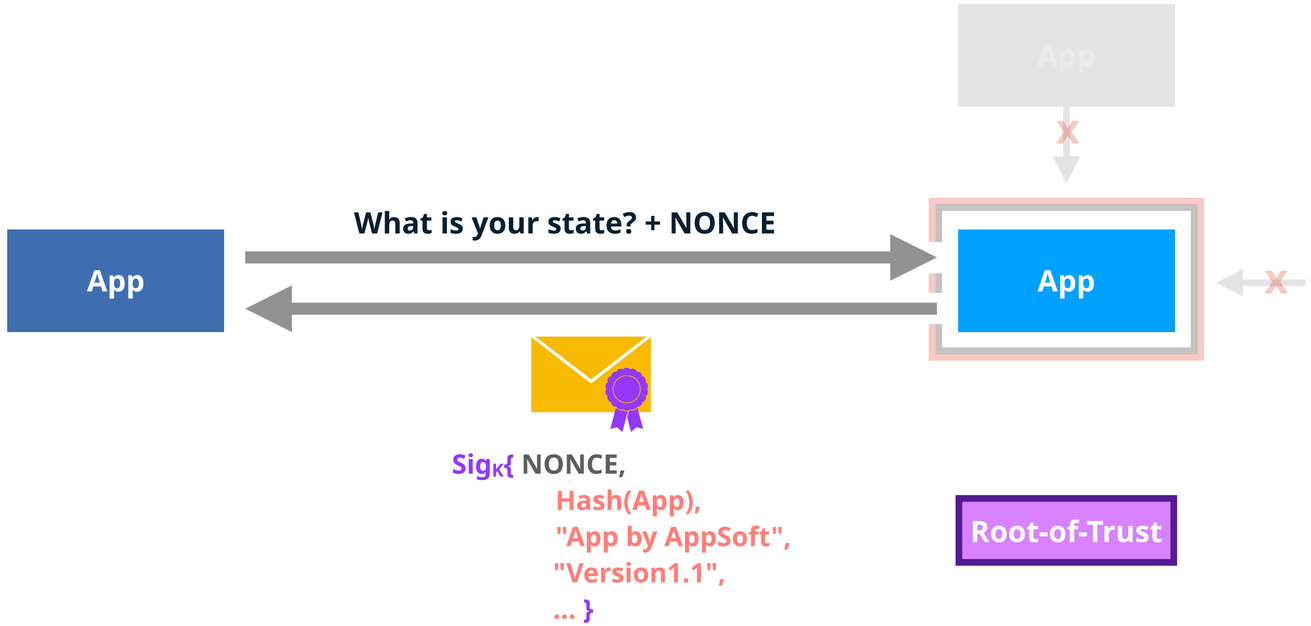
Towards Modular Trusted Execution Environments,
Carsten Weinhold, Nils Asmussen, Diana Göhringer, Michael Roitzsch,
6th Workshop on System Software for Trusted Execution (SysTEX), 2023

barkhausen institut

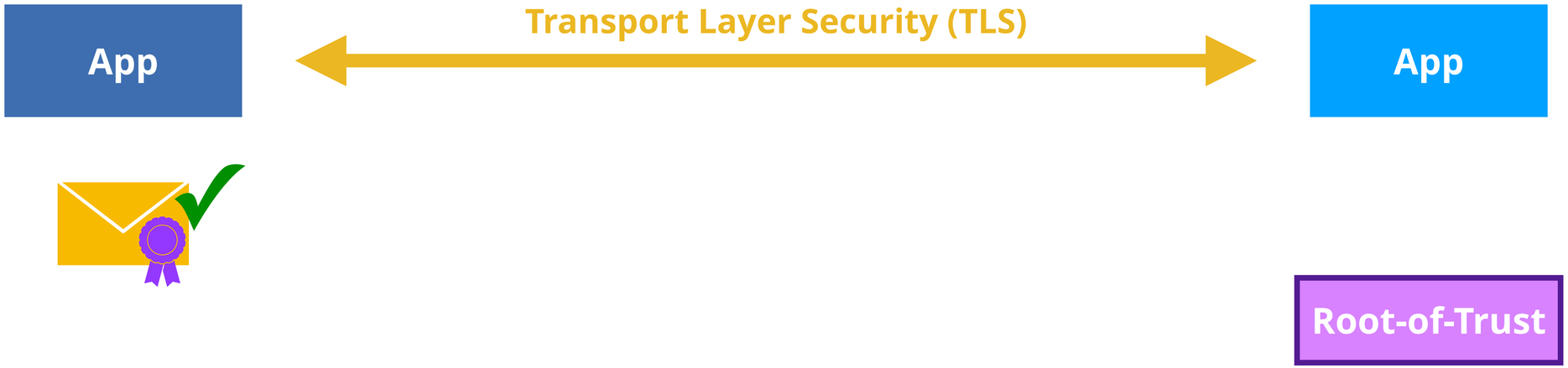
Secure Communication between TEEs

Six Concerns for TEE Design and Implementation

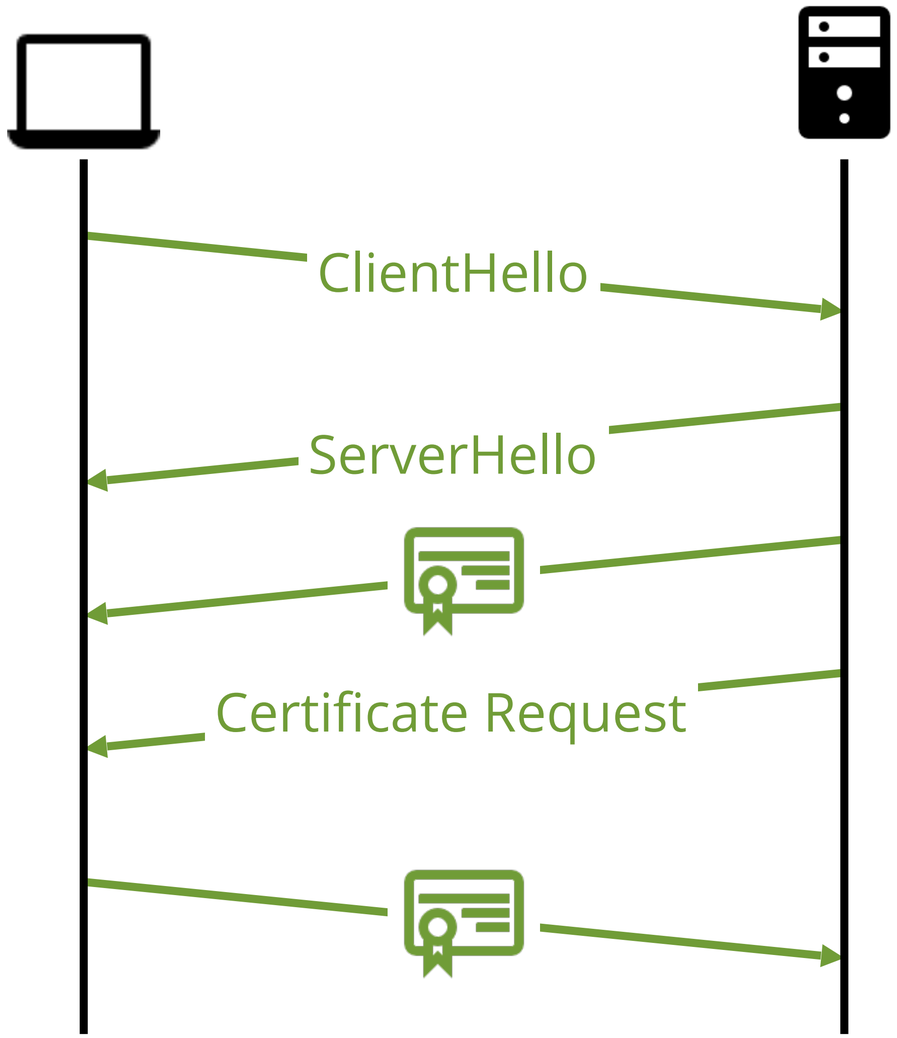
- Computation
- Measurement
- Root of Trust
- Isolation
- Management
- Environment + Communication



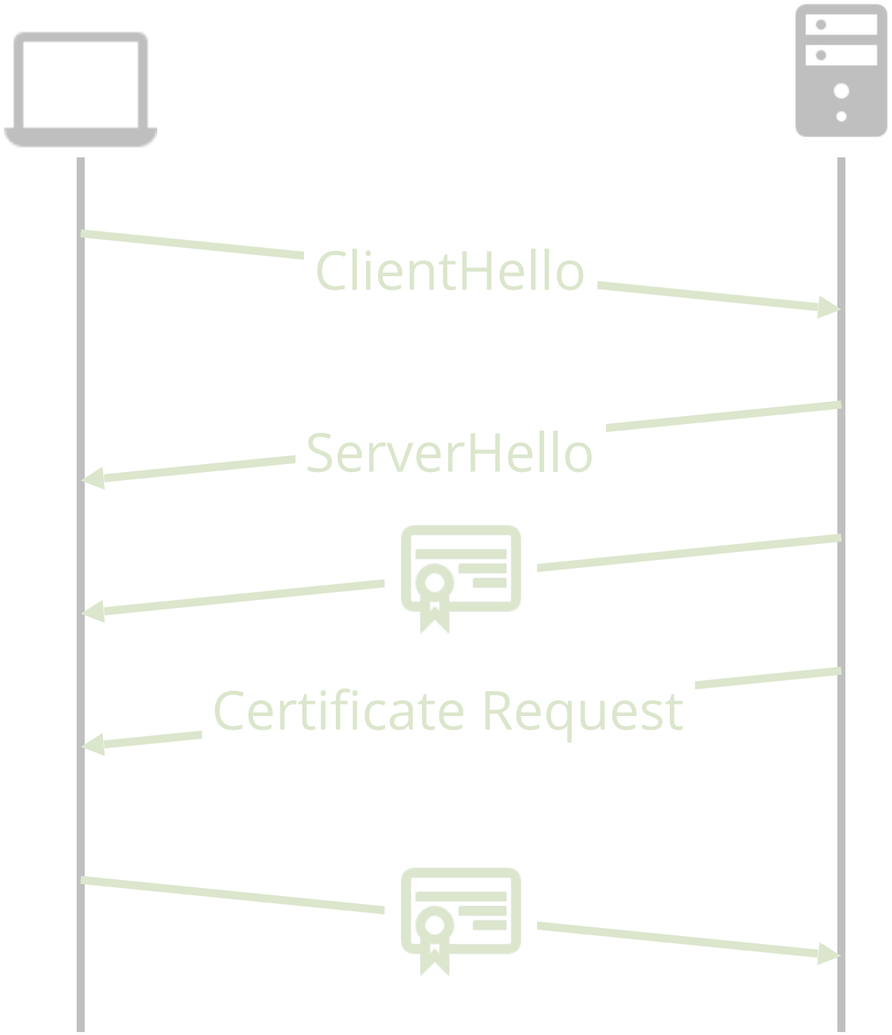
Secure Communication between TEEs

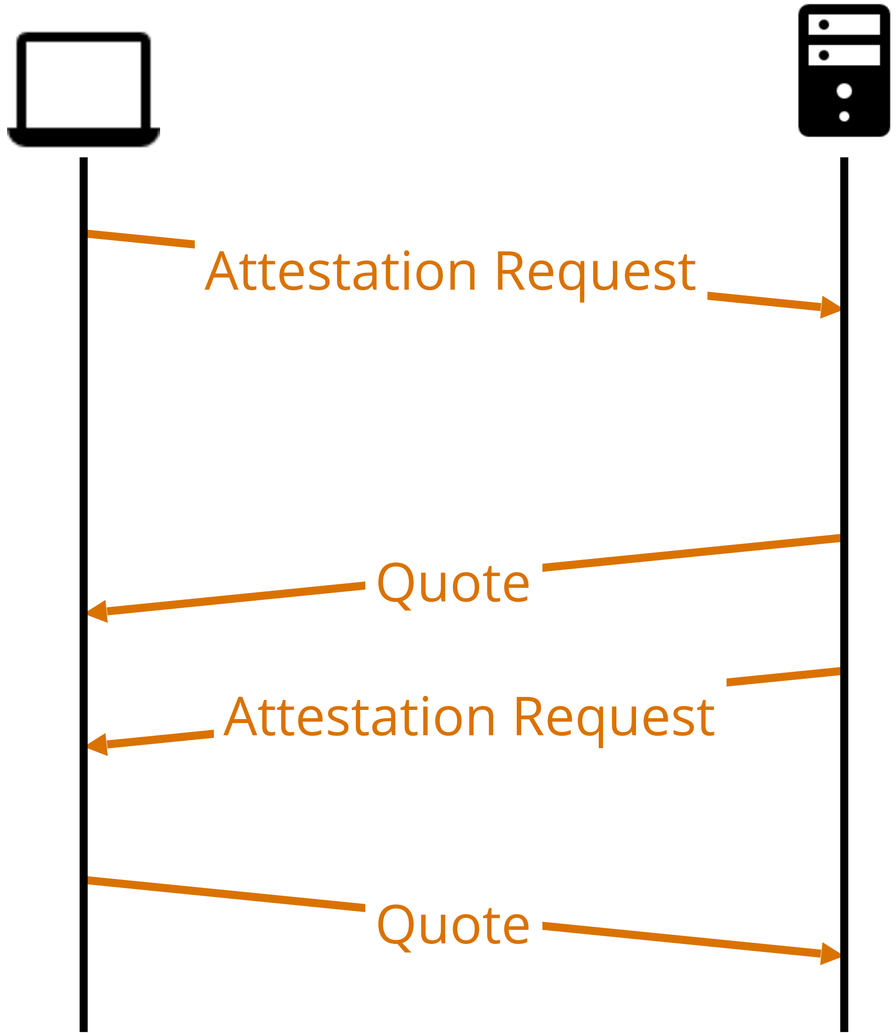


Handshake: Transport Layer Security (TLS)

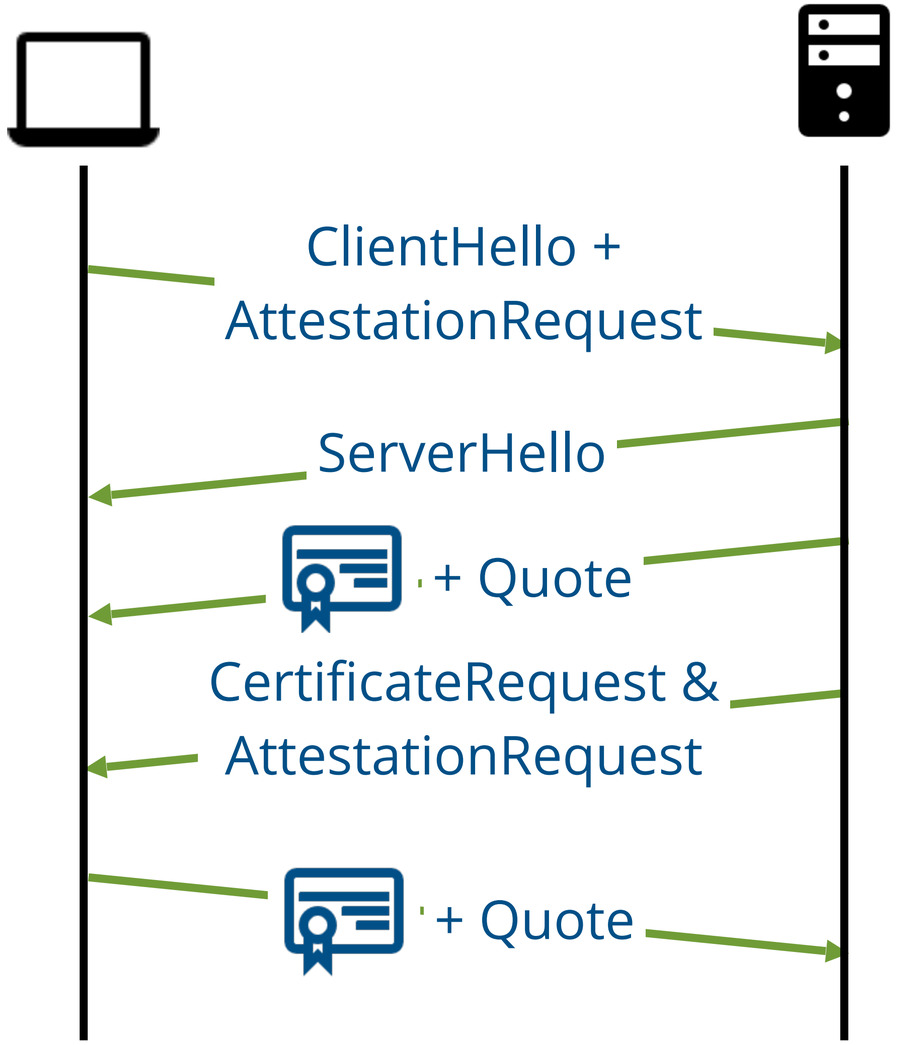


Handshake: Remote Attestation (RA)

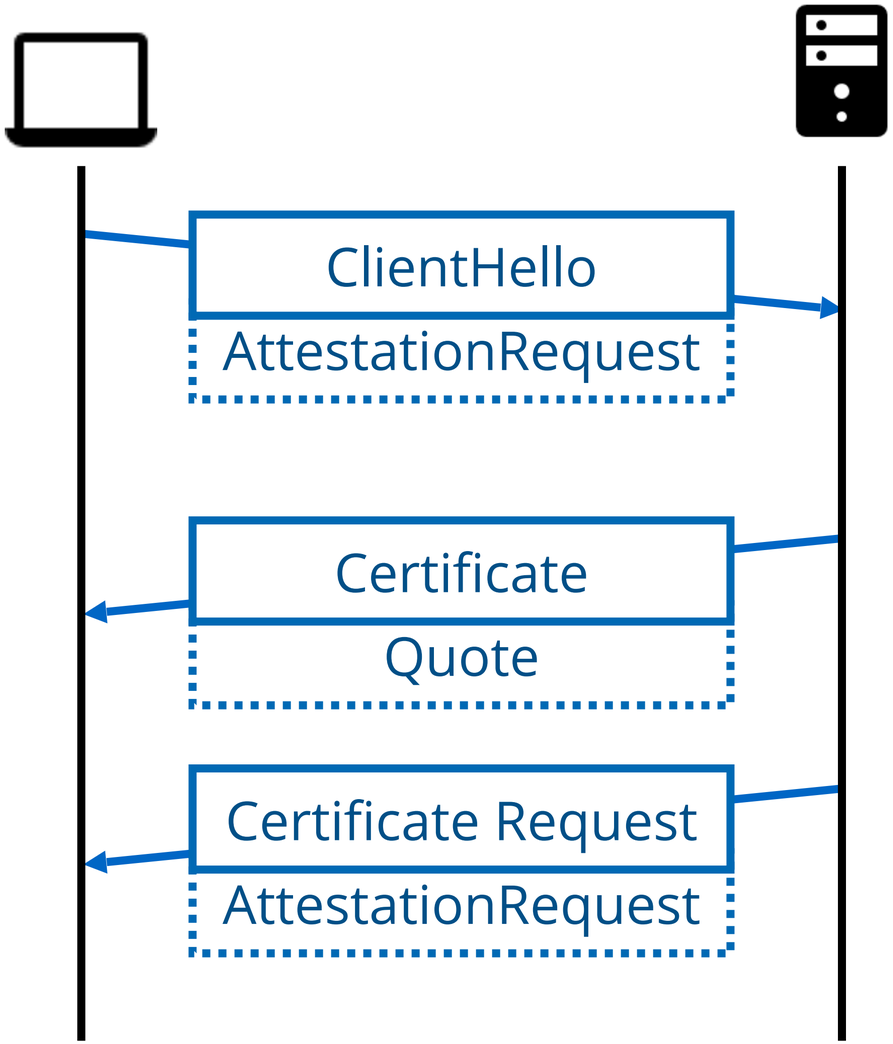


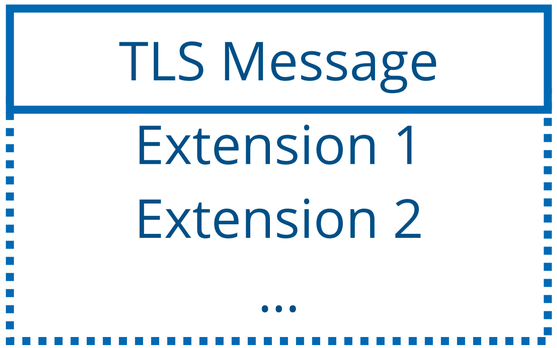


Handshake: TLS+RA



RA piggy-backed in TLS message extensions





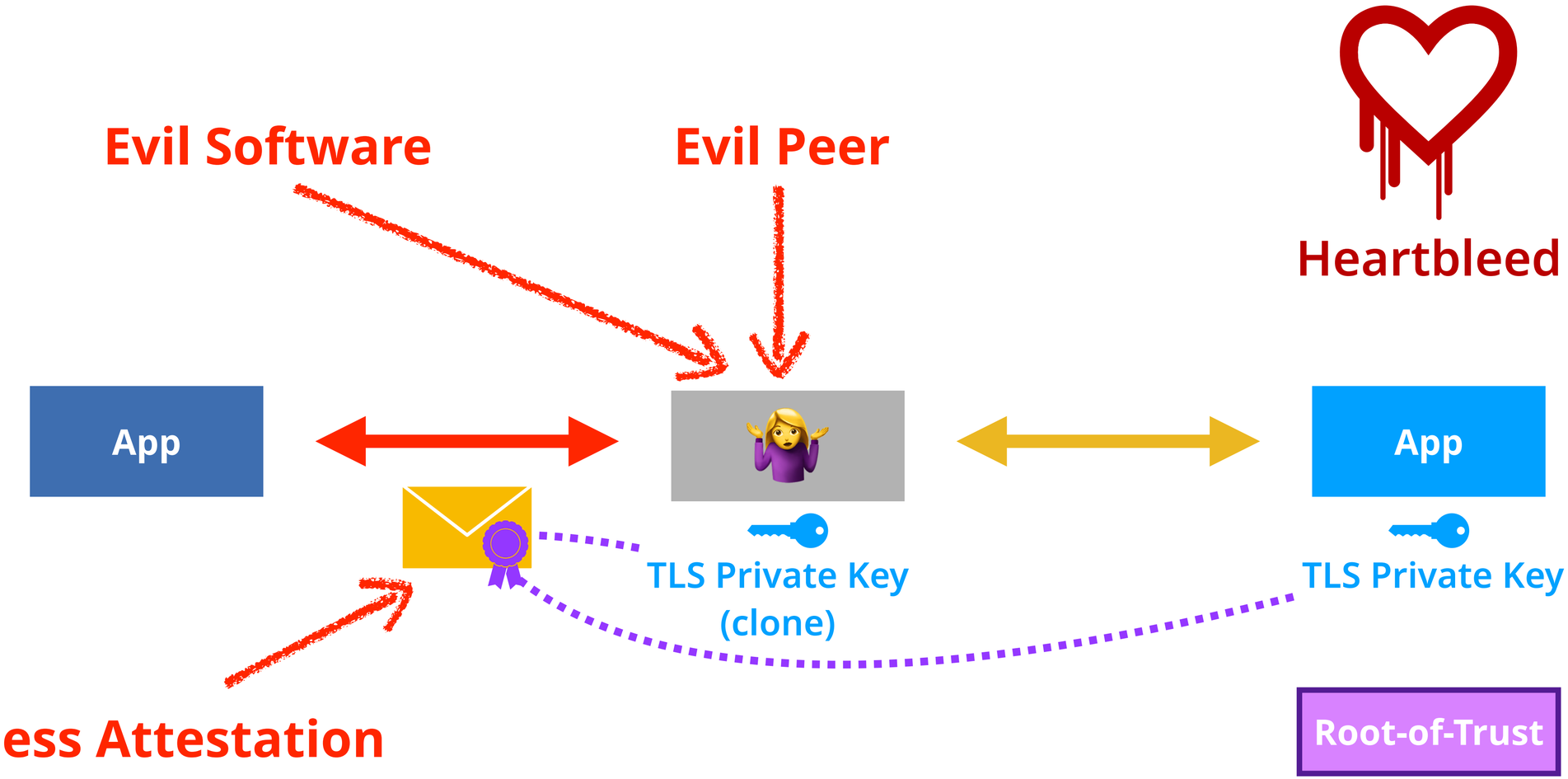
RATLS: Integrating Transport Layer Security with Remote Attestation,
Robert Walther, Carsten Weinhold, Michael Roitzsch,
4th Workshop on Cloud Security and Privacy (Cloud S&P), 2022

Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS),
Hannes Tschofenig, Yaron Sheffer, Paul Howard, Ionuț Mihalcea, Yogesh Deshpande,
Arto Niemi, Thomas Fossati,
IETF Draft, last updated 2024-03-19,
https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/

Combining TLS and RA

	No added round trips	No added encryption
HTTPA		
Platform Certificate	✓	✓
RA-TLS	✓	✓
RA-TLS with CA		✓
Extending TLS		✓
RATLS	✓	✓
Trusted Channels	✓	✓

Relay Attacks

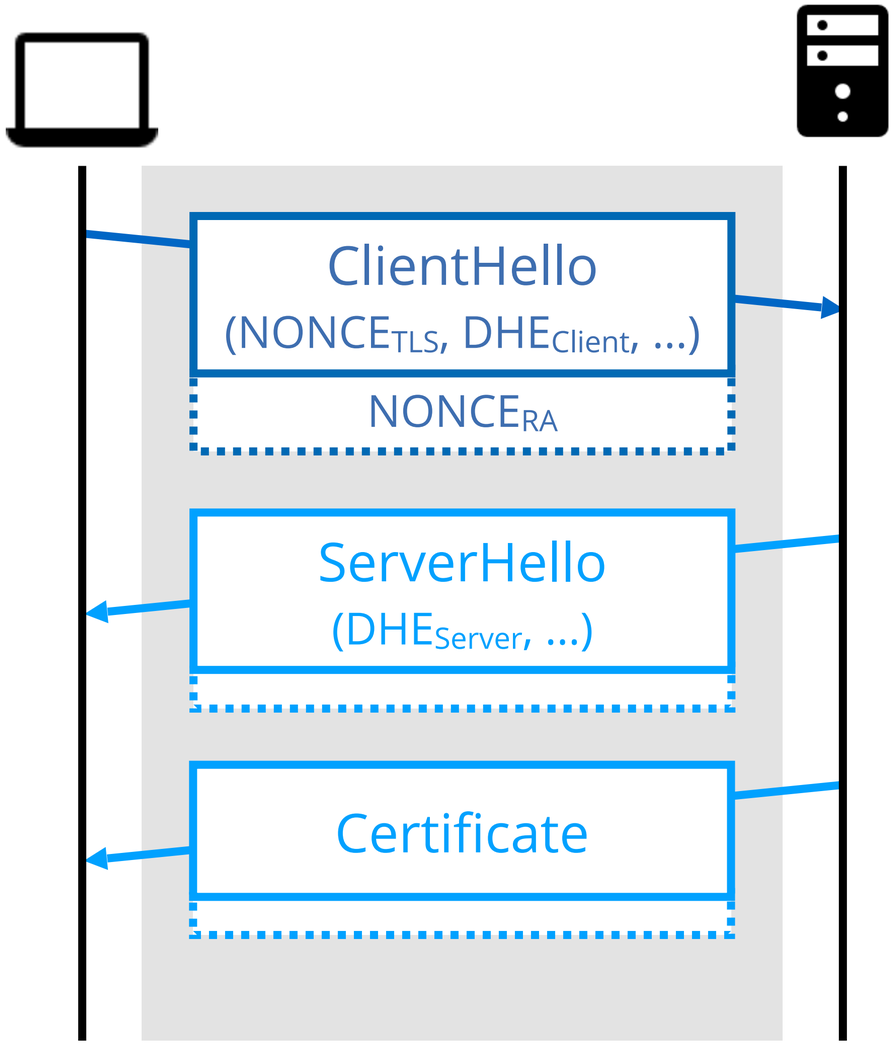


Compromising TLS "breaks" Attestation, too!

Combining TLS and RA

	No added round trips	No added encryption	Prevents Relay Attacks	Independent failure
HTTPA			✓	✓
Platform Certificate	✓	✓	✓	
RA-TLS	✓	✓	✓	
RA-TLS with CA		✓	✓	
Extending TLS		✓	✓	✓
RATLS	✓	✓	✓	
Trusted Channels	✓	✓	✓	

TLS+RA: DHE Shared Secret and Handshake Transcript

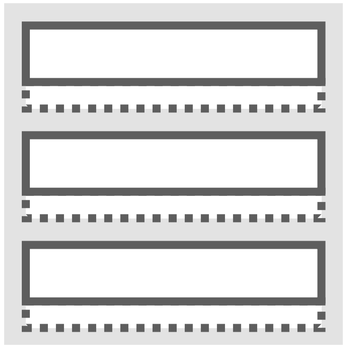


Ephemeral Diffie-Hellman Key Exchange:

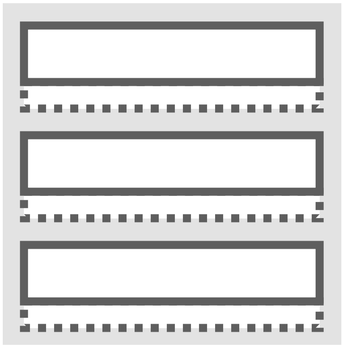
Client: DHE := DHE$_{Client_private}$ • DHE$_{Server}$

Server: DHE := DHE$_{Server_private}$ • DHE$_{Client}$

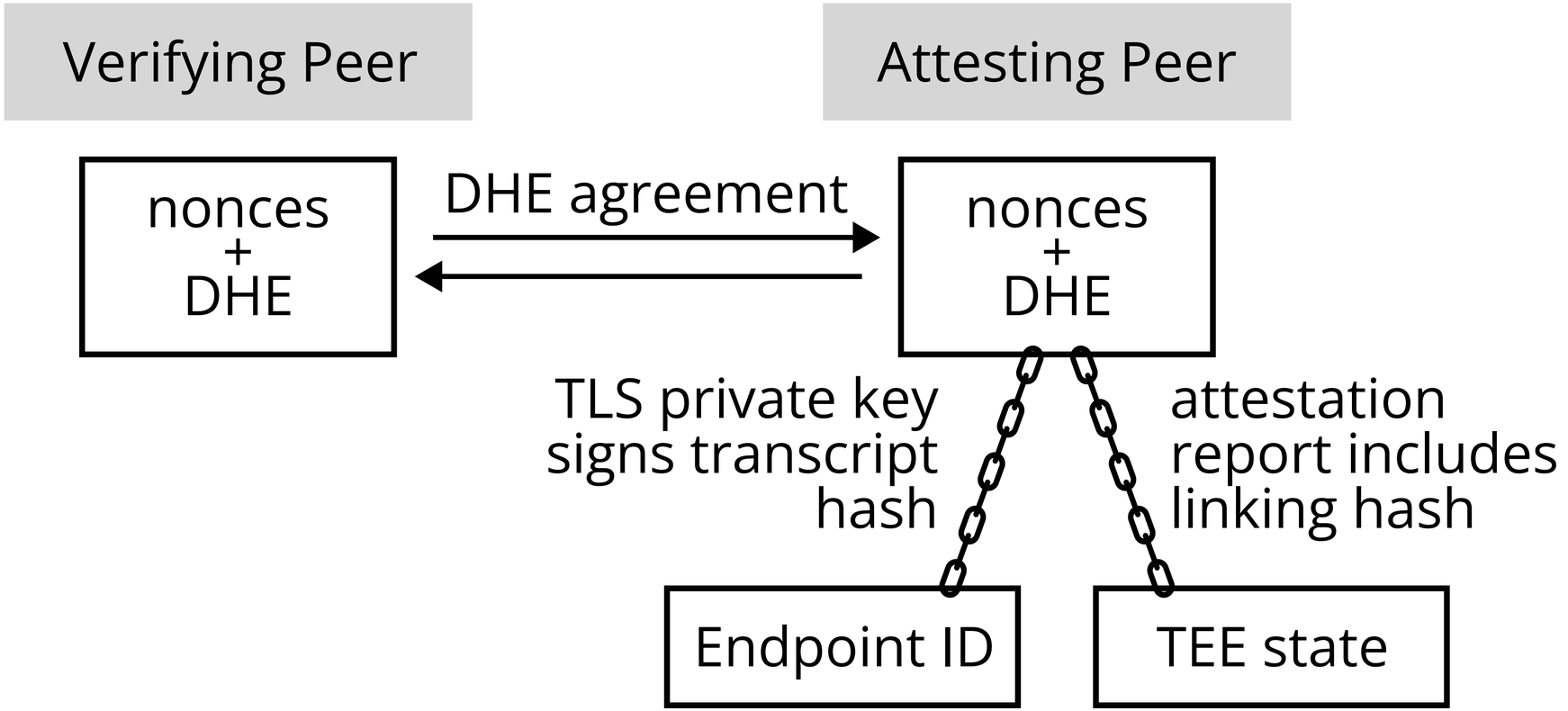
Transcript hash:

H()

Linking hash:

H(
DHE)

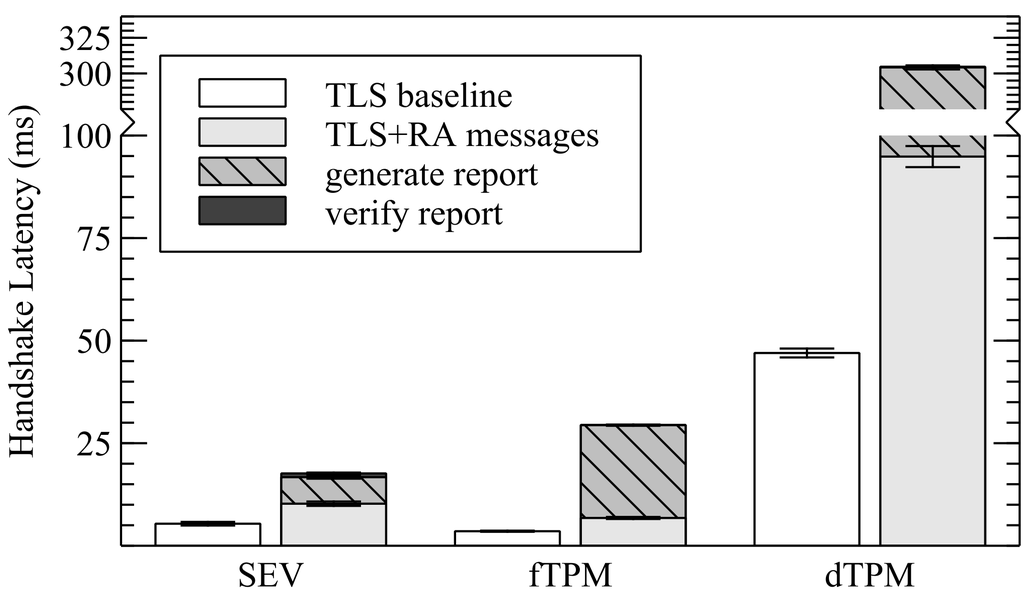
TLS+RA: Additive Security

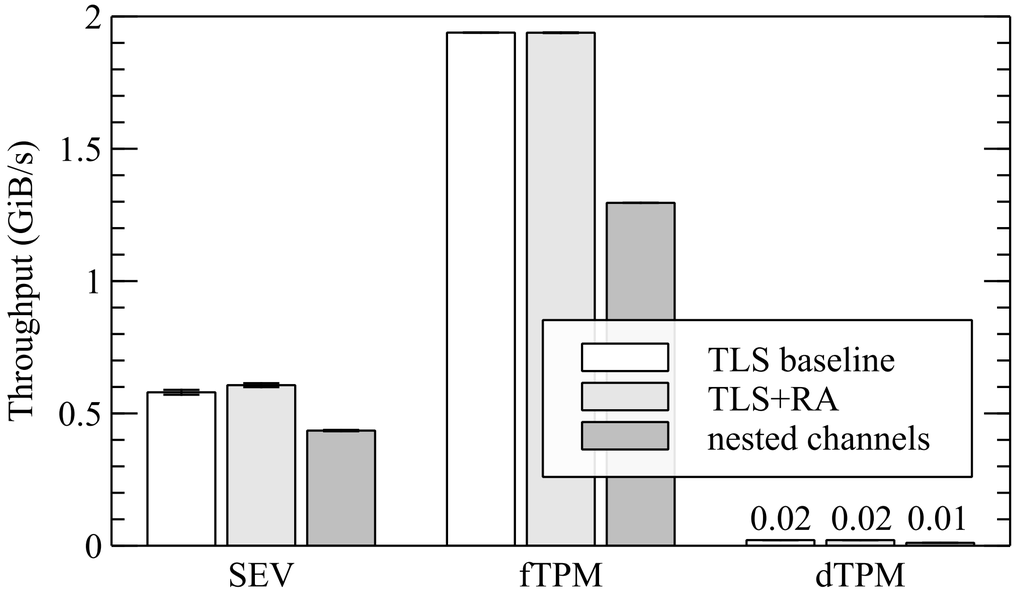


Combining TLS and RA

	No added round trips	No added encryption	Prevents Relay Attacks	Independent failure	Independent deployment
HTTPA			✓	✓	✓
Platform Certificate	✓	✓	✓		
RA-TLS	✓	✓	✓		
RA-TLS with CA		✓	✓		
Extending TLS		✓	✓	✓	
RATLS	✓	✓	✓		✓
Trusted Channels	✓	✓	✓		✓
TLS+RA	✓	✓	✓	✓	✓

TLS+RA: Performance





Summary

- **TEEs** should be modular
- **TLS+RA** is modular, too:
  - Message extensions
  - Independent of root-of-trust
  - Independent deployment
  - Independent failure
- **TLS+RA** provides **additive security**