ICRI-CARS
Secure Systems Group, Aalto University

Lachlan J. Gunn, Ricardo Vieitez Parra, N. Asokan

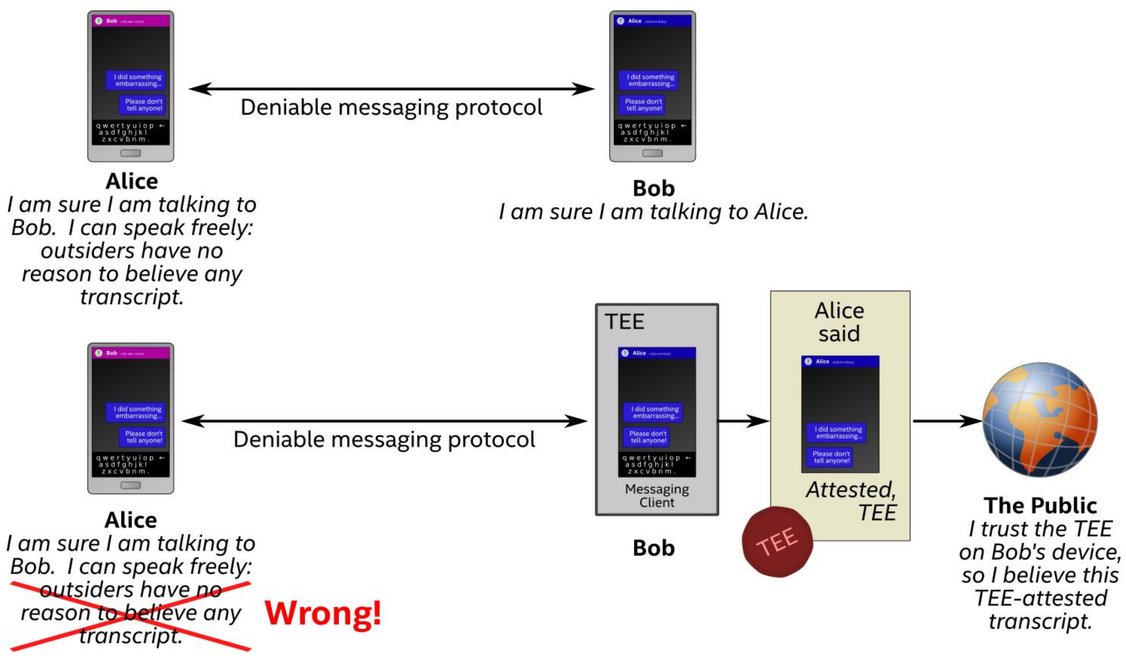
Breaking and repairing deniable messaging using remote attestation

1. What is deniability and why does it matter?

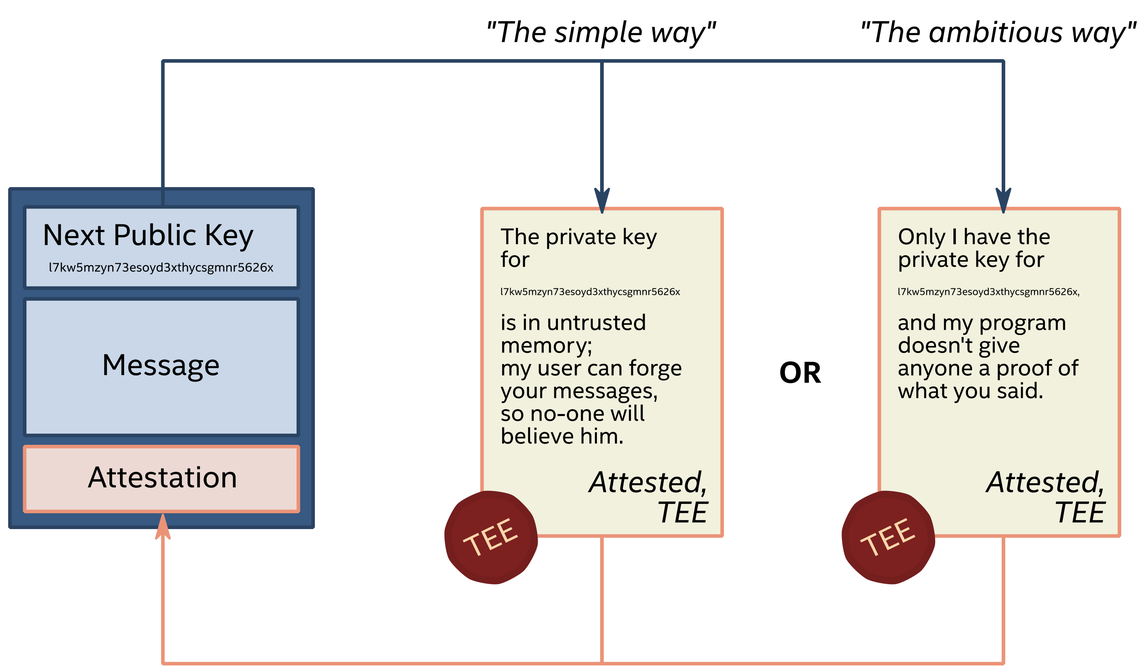
- A deniable protocol lets you prove that a message came from you, such that the recipient cannot prove this to anyone else.
- Email is not deniable because it is often signed by mailservers for anti-spam purposes.
- Non-deniable messages are dangerous: The public can verify leaked emails without needing to trust the source of the breach.
- Deniable protocols are now a target: Many politicians use deniable messenger apps like WhatsApp, Signal, and Telegram.

2. How does attestation break deniability?

- Authentication: Deniable protocols can still authenticate.
- Attestation: Attestation of a messaging protocol output provides a proof of what was said.
- Any authenticated protocol: Applies to messaging, email, online chat, etc.
- Undetectability: This proof does not change the messaging protocol, so is undetectable.
- Remote attacks are possible: A compromised device can use its TEE to produce these attestations for newly-received messages.



An attacker can use the trusted execution environment in Bob's phone to convince others of what they found.



We can defeat this attack against Signal by including an attestation against each public key, showing who can verify messages authenticated using it.

3. How does this attack work in practice?

- Signal inside SGX: We have produced an enclave implementing the cryptographic functionality for the Signal protocol.
- Log received messages: The enclave logs all messages received, along with the identity of their source.
- Attest to the log: At the end of the session, the enclave produces an attestation to the hash of the log.
- Undetectability: The protocol does not change, so the victim knows nothing.

4. How can attestation restore deniability?

- In general: Bob's TEE attests to Alice that no meaningful attestation of their conversation is possible.
- The simple way: Attest that authentication keys were exported outside this TEE, making messages forgeable by Bob.

  Small TCB: easy to verify, but we lose other benefits of a TEE.
- The ambitious way: Put the whole client inside the TEE and attest that it will only output cleartext messages.

  Large TCB: hard to verify, but the TEE can protect keys.
- Hypothesis: this approach can protect against online attacks, making Signal more deniable than it was originally.

Aalto University
Research Institute for Collaborative Autonomous and Resilient Systems
ia.cr/2018/424