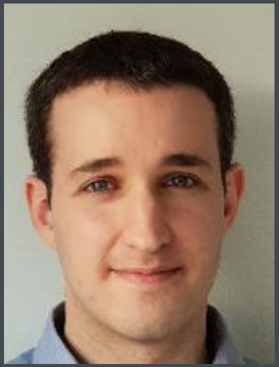
Exported Authenticators

Cas Cremers
University of
Oxford



Jonathan Hoyland
Royal Holloway,
University of
London

A Formal Analysis

ROYAL HOLLOWAY UNIVERSITY OF LONDON

IETF 101: 21 March 2018

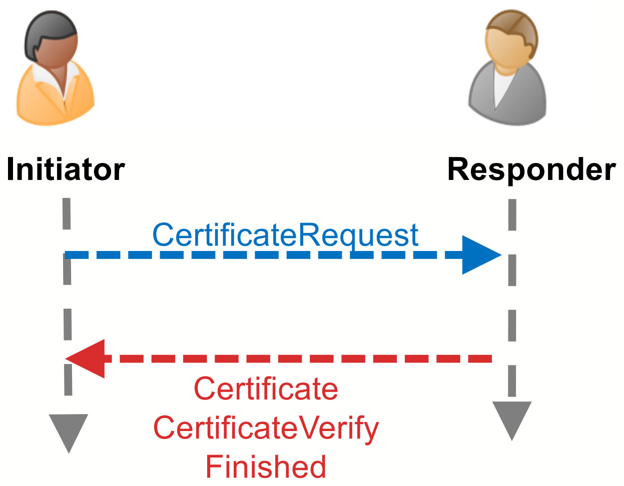
Exported Authenticators

- Post-handshake authentication mechanism.
- Replacement for TLS 1.2’s renegotiation.
- More versatile than TLS 1.3’s post-handshake client authentication
- Allows multiple identities for both the Client and the Server.

Draft-Sullivan Flows

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Request/Response EA



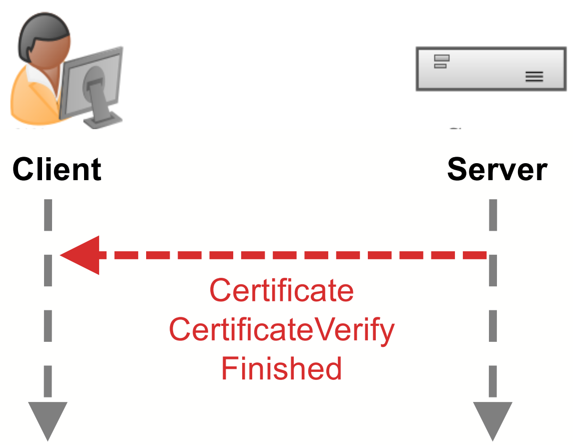
Initiator

Responder

CertificateRequest

Certificate
CertificateVerify
Finished

Spontaneous EA



Client

Server

Certificate
CertificateVerify
Finished

Security Considerations

EA must prove control of certificate to peer

- Attacker must not be able to produce an EA without access to the certificate’s private key.
- EAs must be fresh.

EA must prove control of the TLS channel

- Attacker must not be able to attribute an EA to a channel other than the one for which it was created.

Compound Authentication

IF: a run of layered authentication protocols completes,

AND: at least one peer identity is uncompromised,

THEN: you know the peer agrees on all identities and bindings.

Formal Analysis

We perform an analysis in two parts:

Proof by hand

- Used channel bindings framework
- Proved compound authentication

Tool-supported proof

- Built a Tamarin model
- Explored draft-Sullivan’s security guarantees

Manual Proof

Used channel bindings as a framework to analyse EAs.

Numerous examples of layered protocols in the literature that fail to achieve compound authentication.

Contributive channel bindings[1] can be used to formally verify compound authentication.

[1] Bhargavan, K., Delignat-Lavaud, A., & Pironti, A. (2015, February). Verified Contributive Channel Bindings for Compound Authentication. In NDSS.

Tool-Assisted Proof

Used Tamarin[2], a formal protocol verification tool.

Used to analyse TLS 1.3 symbolically.

Can prove complex and nuanced security properties.

We used it to explore various properties and threat models.

Can be used to find counter-examples for properties that do not hold.

[2]https://tamarin-prover.github.io/

Results of Overall Analysis

The TLS channel and the EA are securely bound, and achieve compound authentication

- To forge an EA the attacker must know the master secret of the TLS channel AND the private key of the certificate.

If the master secret is uncompromised then the authentication of two EAs are bound to each other.

Threat Model Exploration

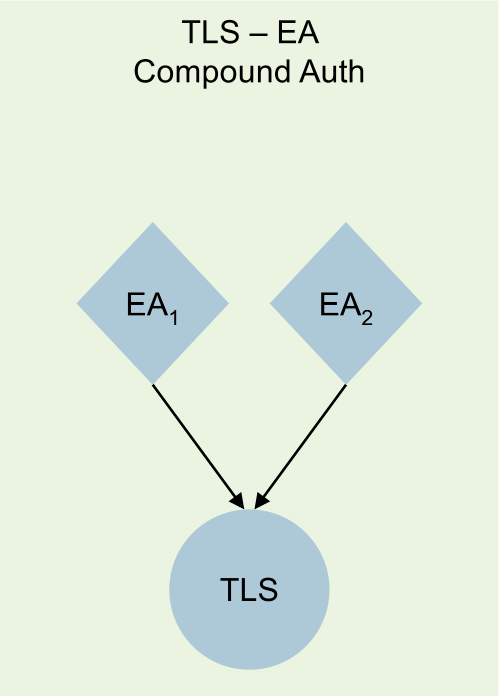
ROYAL HOLLOWAY UNIVERSITY OF LONDON

How far can we push the threat model before something breaks?

- Attacker can compromise the master secret and knows some private keys.
  - EAs are not separately bound to each other.
  - Can’t guarantee that all EAs came from the same actor.
  - We’re working on a stronger version.
- Is this threat model plausible?
  - The master secret could exported by the server to enable visibility.
  - Overseer could insert EAs onto a connection in either direction.

E-mail me: Jonathan Hoyland jonathan.hoyland@gmail.com

Compound Authentication



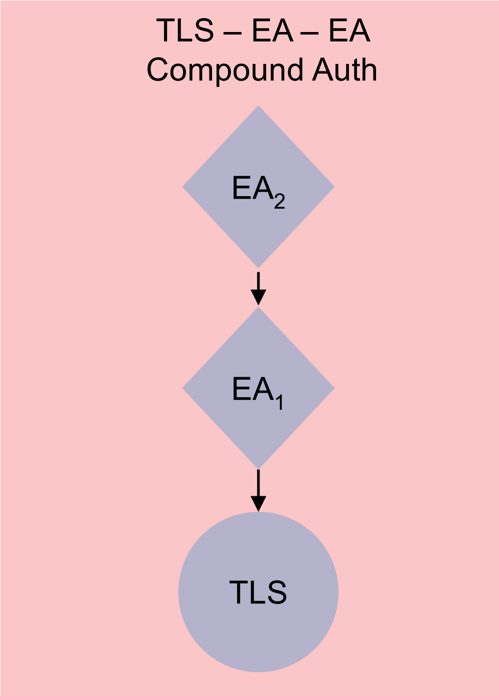
TLS – EA
Compound Auth

EA_1

EA_2

TLS

What we Proved



TLS – EA – EA
Compound Auth

EA_2

EA_1

TLS

What we are working on