TLS: Transport Layer Security

Véronique Cortier

TLS

- One of the most widely deployed cryptographic protocol : HTTPS, 802.1x, VPNs, mail, VoIP, ...
- Many implementations : SChannel, OpenSSL, NSS, GnuTLS, JSSE, PolarSSL
- many patches every year
- many attacks : Heartbleed, POODLE, RC4, FREAK, Logjam...

$\rightarrow$ 20 years of attacks, fixes, new versions, and extensions

Handshake

1. The client and the server exchange a fresh session identifier.

Handshake

1. The client and the server exchange a fresh session identifier.
2. The client and the server negotiate :
   - which key exchange protocol to use (e.g. RSA, DH, DH-static, ...)
   - encryption mode : MAC&ENCRYPT, RC4, ...

Handshake

1. The client and the server exchange a fresh session identifier.
2. The client and the server negotiate :
   - which key exchange protocol to use (e.g. RSA, DH, DH-static, ...)
   - encryption mode : MAC&ENCRYPT, RC4, ...
3. The client and the server establish a master session key used to derive session keys.
   - The server may be authenticated (or not)
   - The client may be authenticated (or not)

In general, the server is authenticated, not the client.

Agility

An extremely agile protocol

- a wide choice of algorithms (key-exchange protocols, encryption mode) ;
- very flexible in terms of who is authenticated ;
- possibility to authenticate afterwards.
  Example : a client browses anonymously some web pages and then authenticates to access some service.

Record Layer

Handshake

establishes a key k

Record Layer

uses the key k

The encryption key is passed to the Record Layer even if the authentication is not completed yet.

Key changes

Resumption : Change of the session key, derived from the master key
$\rightarrow$ avoids to start the (more costly) asymmetric part.

Key changes

Resumption : Change of the session key, derived from the master key
→ avoids to start the (more costly) asymmetric part.

Renegotiation : Change of the master key
→ various reasons. For example, the client now wishes to be authenticated.

Key changes

Resumption : Change of the session key, derived from the master key
→ avoids to start the (more costly) asymmetric part.

Renegotiation : Change of the master key
→ various reasons. For example, the client now wishes to be authenticated.

In both cases, these exchanges under the Security Layer, with the current session key.

How it works in more details

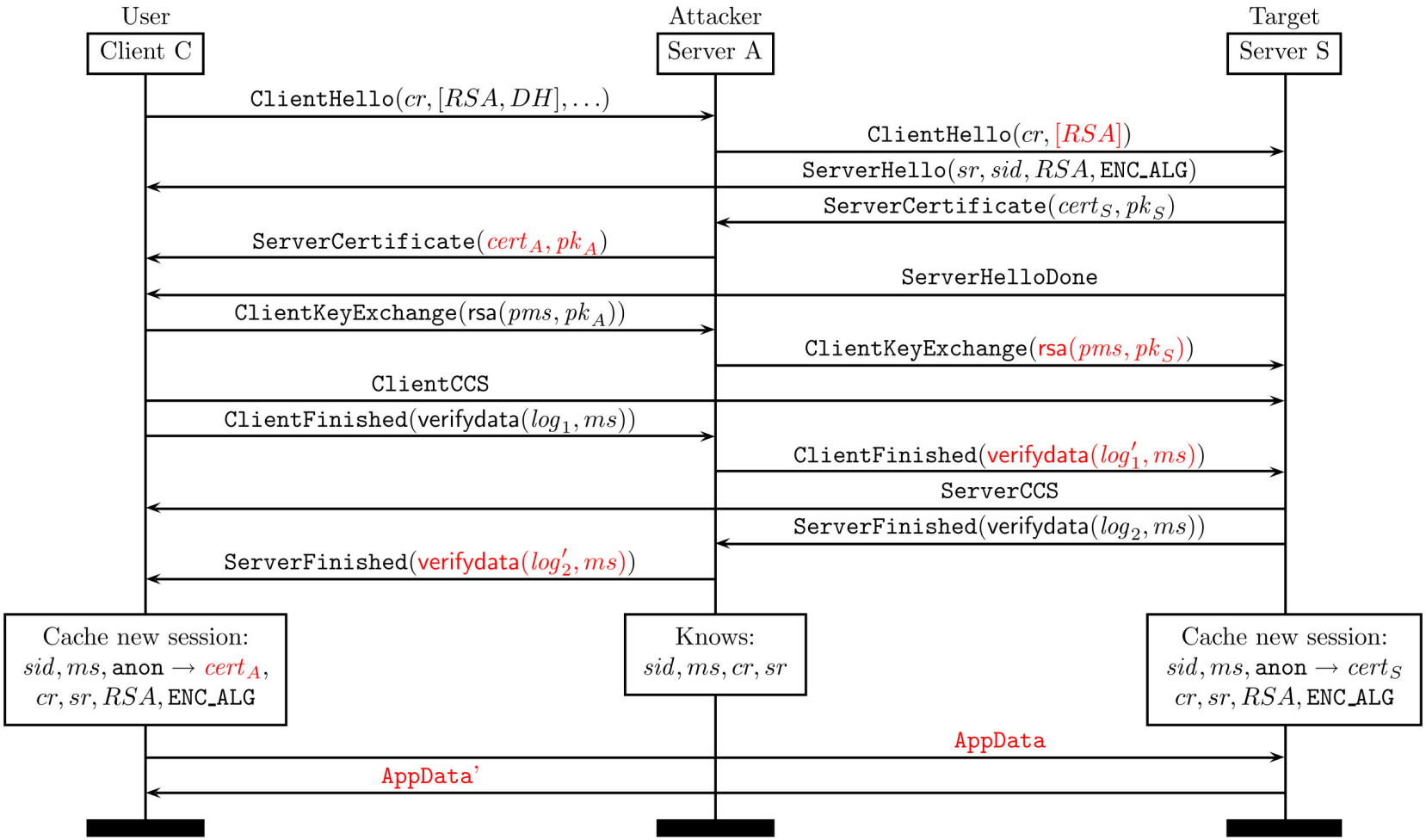
cf course.

Triple Handshake attacks

`https://mitls.org/pages/attacks/3SHAKE`

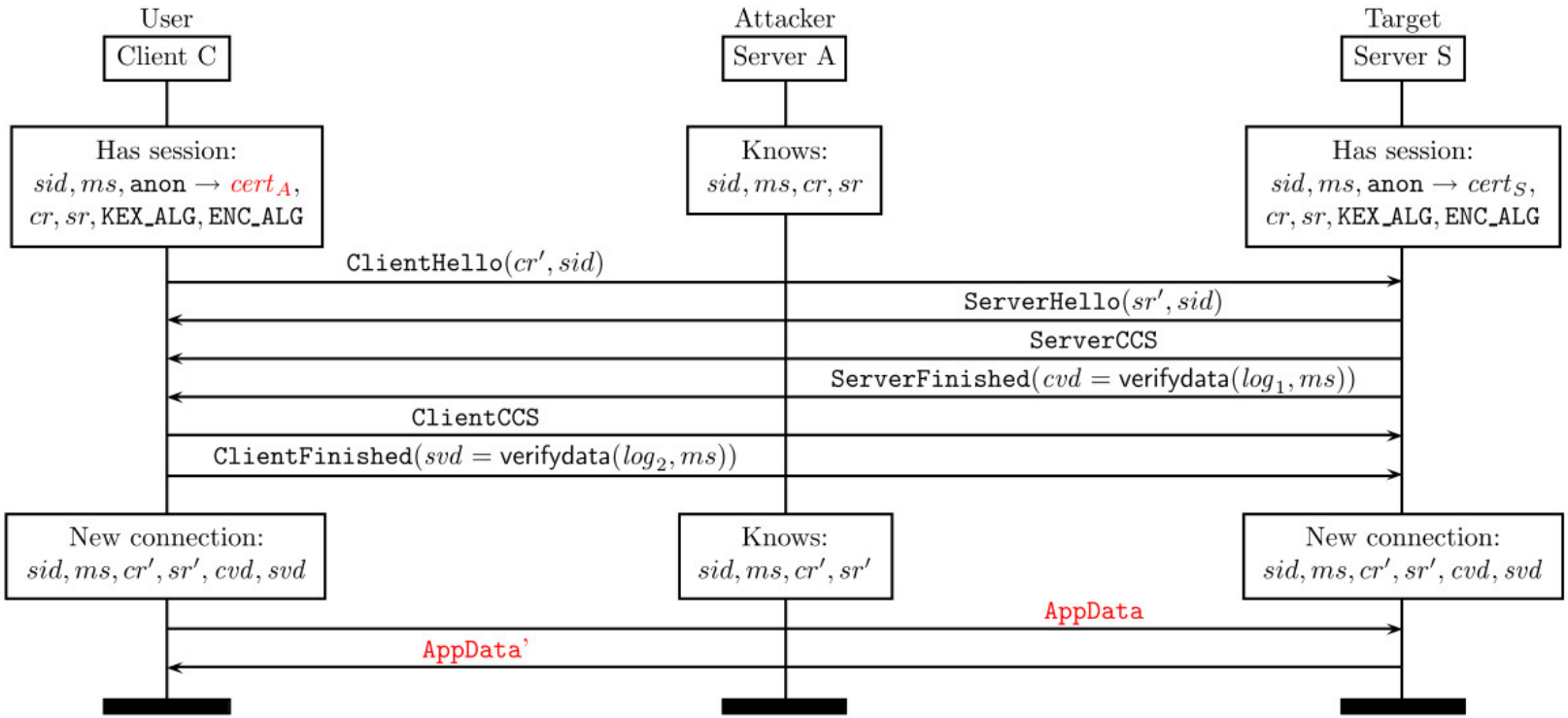
- attack found using formal tools
- authors : Antoine Delignat-Lavaud, Karthikeyan Bhargavan and Alfredo Pironti
  from the Prosecco research team at INRIA Paris-Rocquencourt.
- miTLS research project, aimed at building and verifying a reference TLS implementation.

Phase 1 : Man in the middle



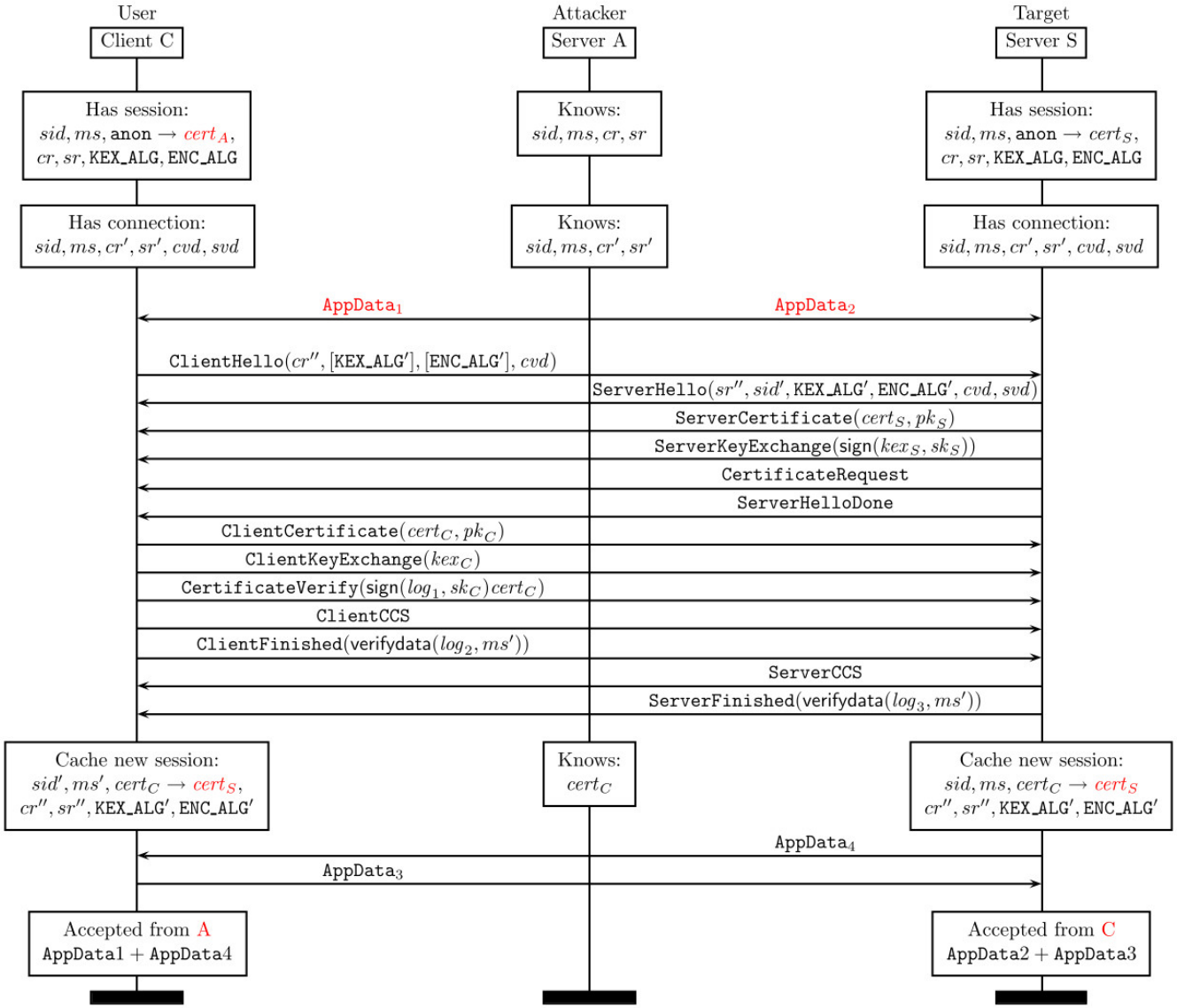
https://mitls.org/pages/attacks/3SHAKE

Phase 2 : Resumption



https://mitls.org/pages/attacks/3SHAKE

Phase 3 : Renegotiation



FREAK attack - February 2015

Bhargavan et al.

LOGJAM attack - February 2015

Adrian et al.