Automated Analysis of TLS 1.3

0-RTT, Resumption and Delayed Authentication

Real World Crypto, 7th January 2016

Cas Cremers

Marko Horvat

Sam Scott

Thyla van der Merwe

UNIVERSITY OF OXFORD

ROYAL HOLLOWAY UNIVERSITY OF LONDON

mozilla

New features of TLS 1.3

What's new in TLS 1.3?

- 0-RTT handshake mode.
- Session resumption merged with PSK mode.
- Delayed client authentication mechanism.
- The full interaction of all the above components, as well as the regular modes.

Objectives

Our goal

Improve the security of TLS 1.3 by analysing the specification using state-of-the-art formal analysis methods.

Challenges:

- Complex protocol.
- Rapidly changing specification.

What class of attacks can we rule out?

Tamarin

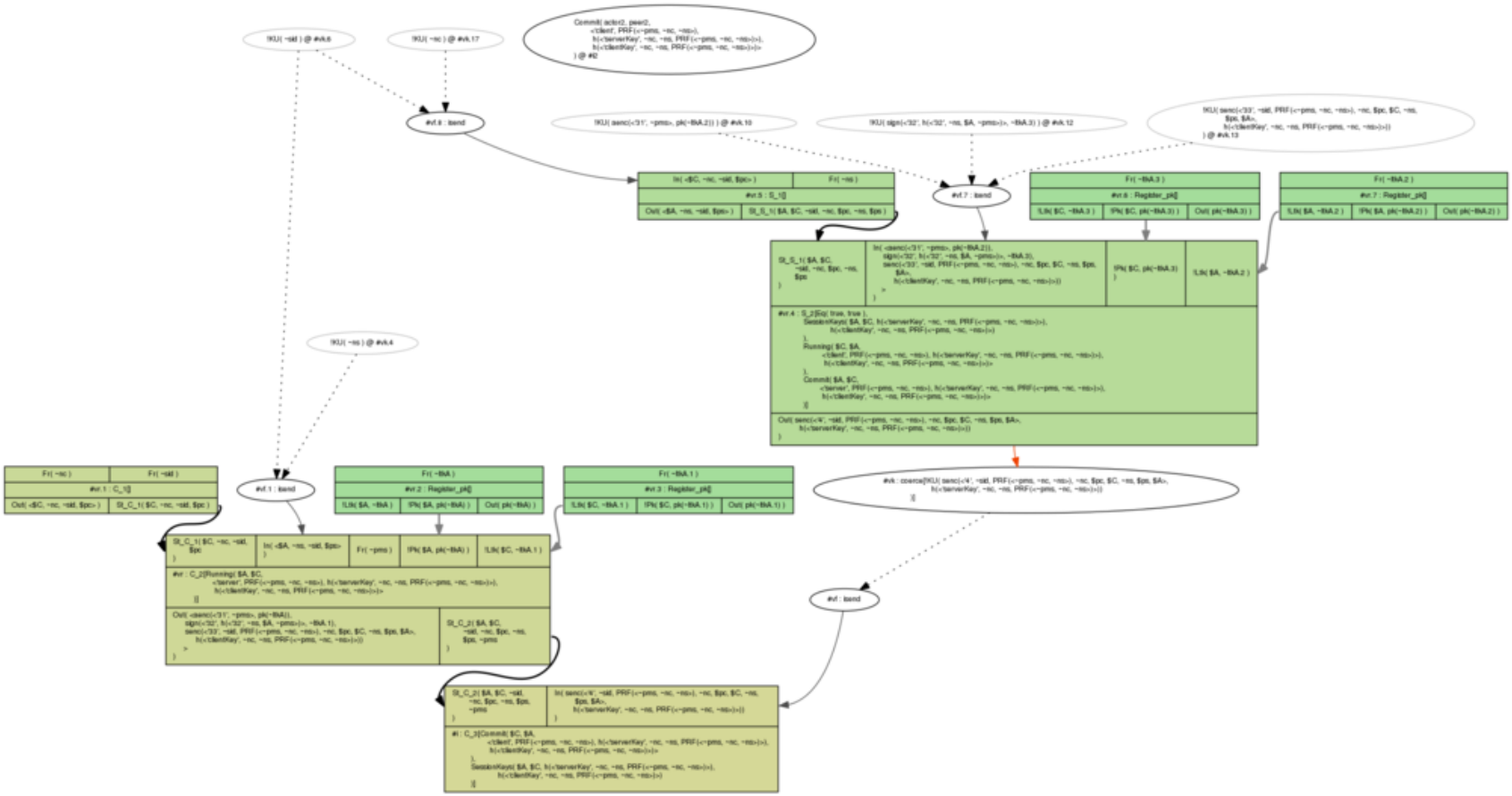
We built our model for use in the Tamarin prover.

- Automated tool for protocol analysis.
- Supports loops and branches.
- Good symbolic Diffie-Hellman support.
- Considers an unbounded number of parties/handshakes.

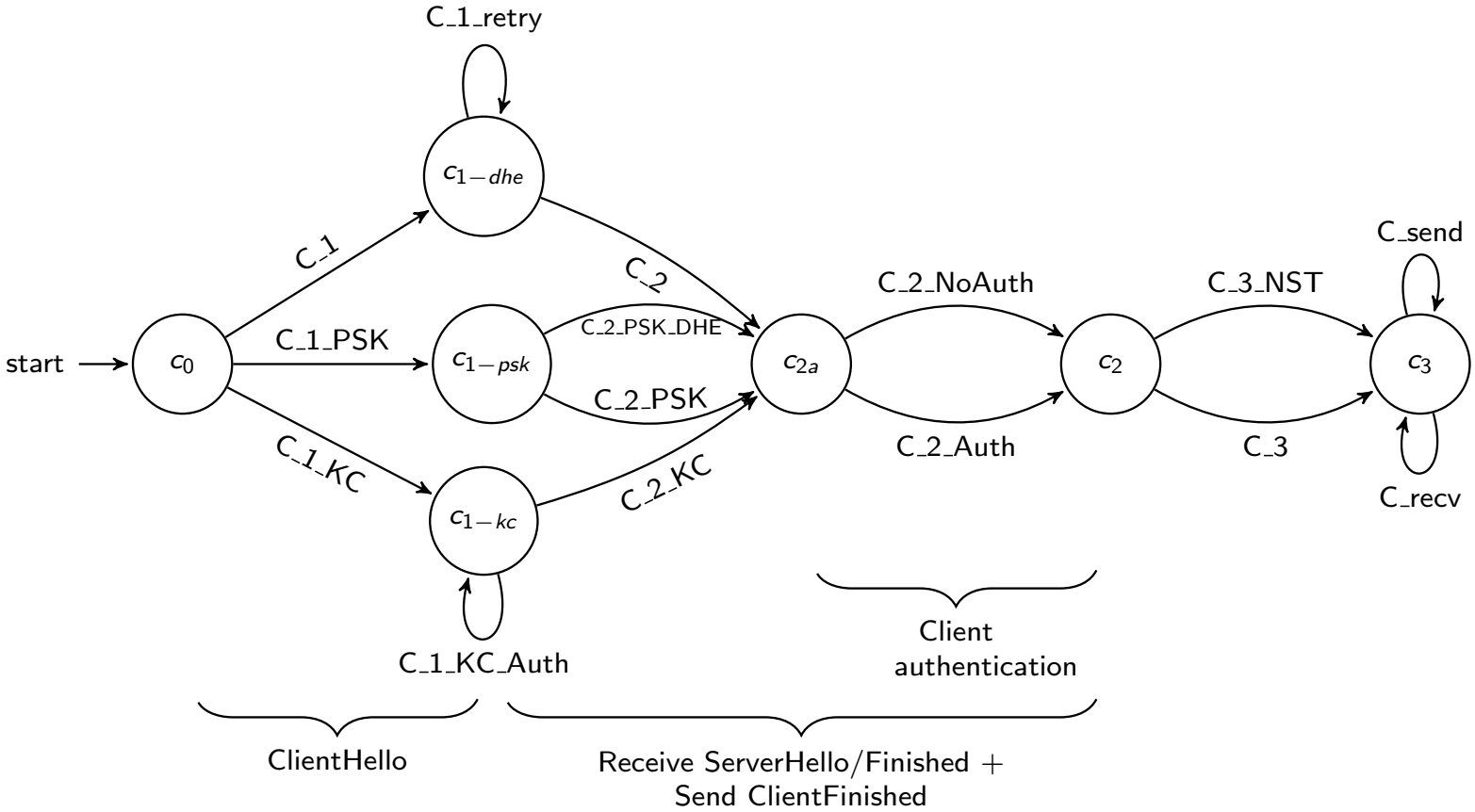
How does it work?

- For simple models/properties, can prove automatically.
- Complex models require more user interaction.
- A proof shows that a property holds in all possible combinations of client, server, and adversary behaviours.

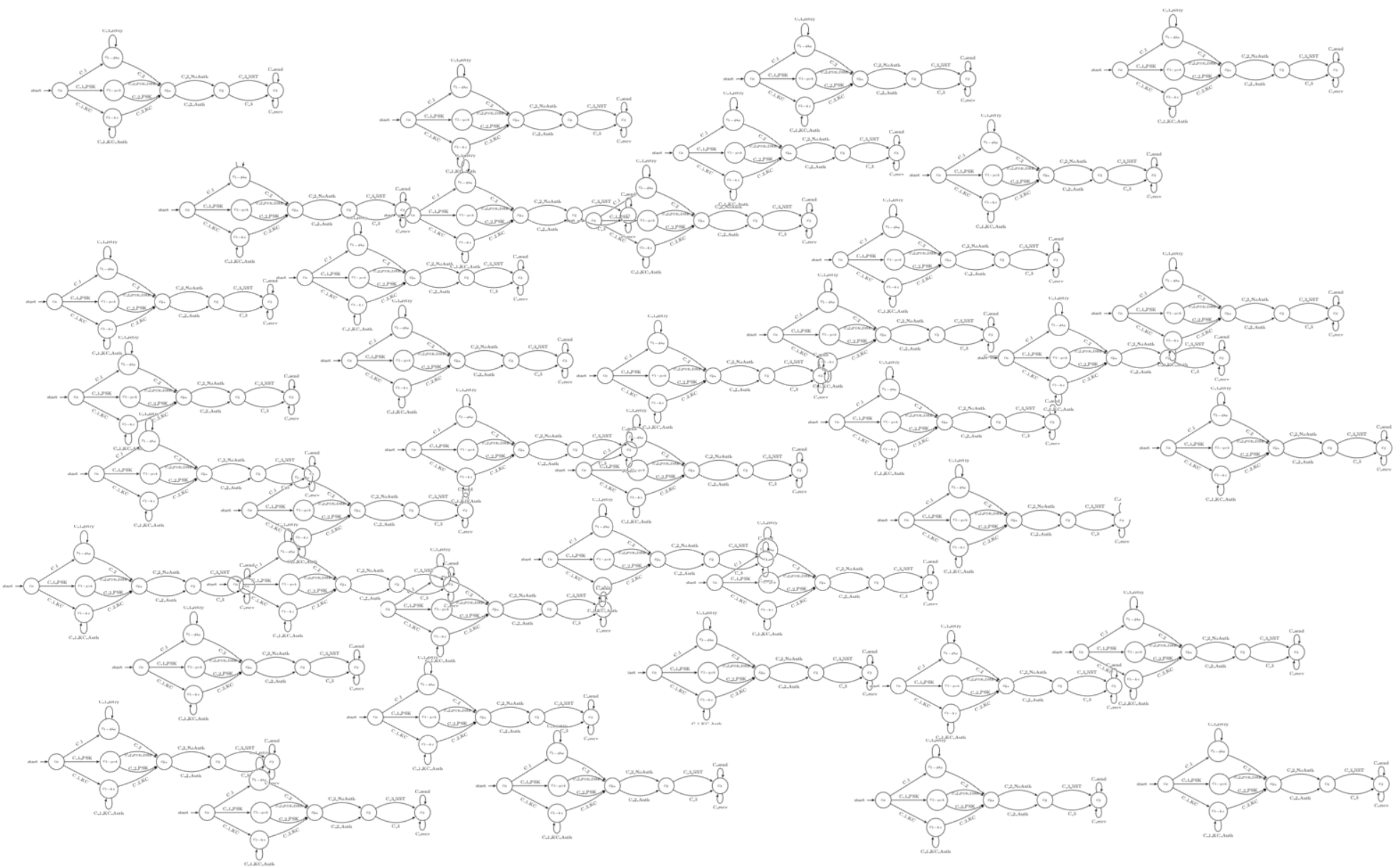
Tamarin



Building a model



Building a model

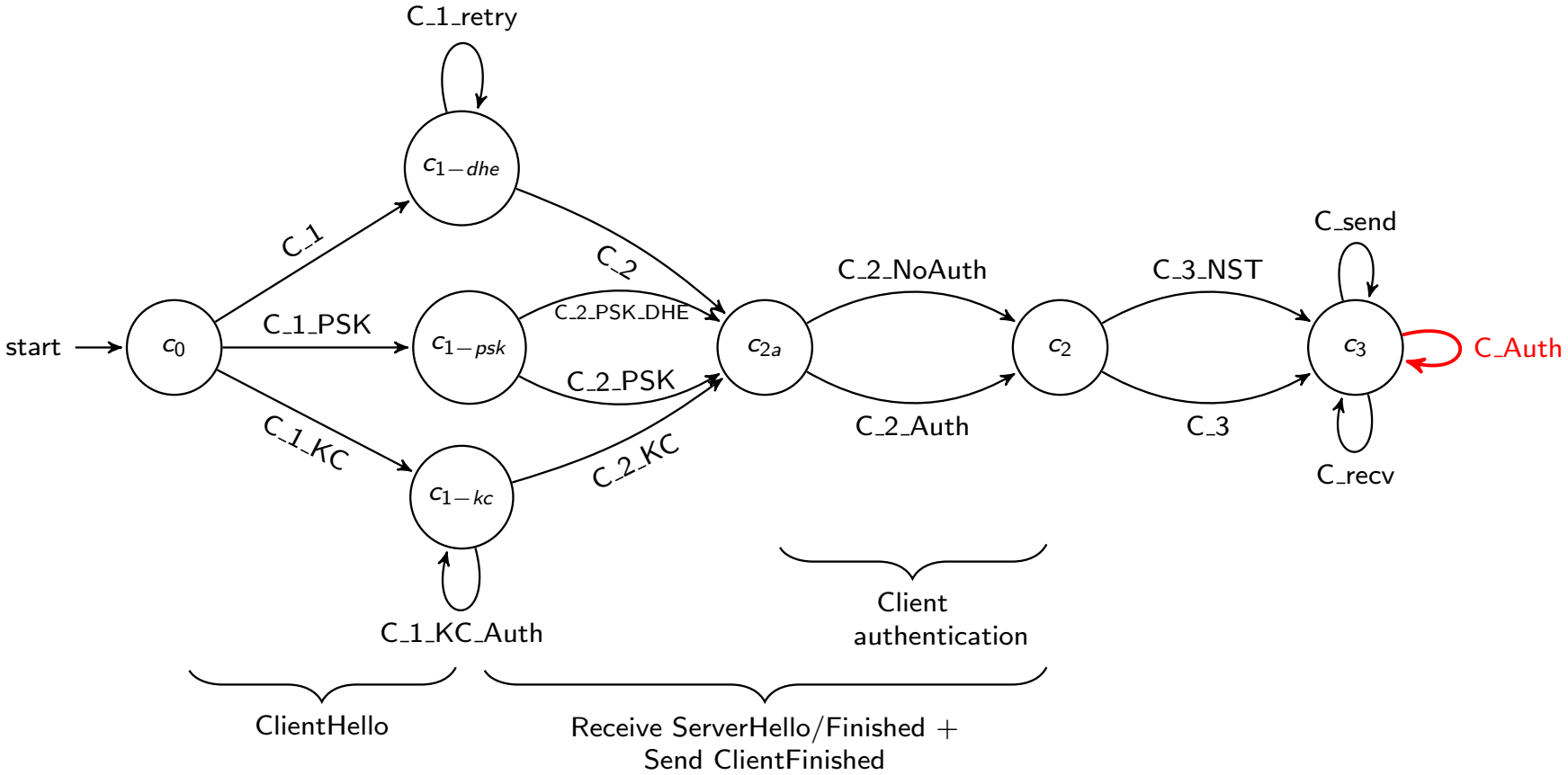


Verification

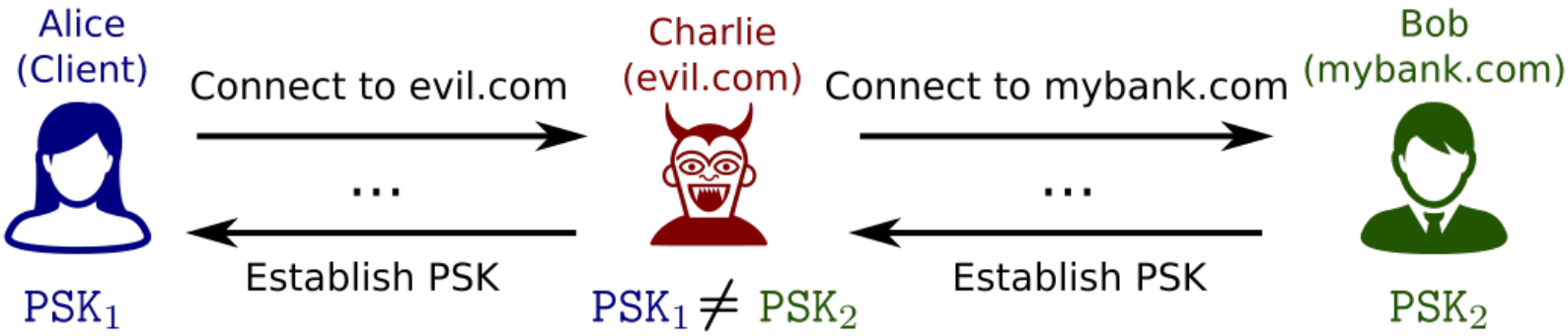
We verified the core properties of TLS 1.3 revision 10 as an authenticated key exchange protocol:

- Secrecy of session keys.
  - Holds for both client and server.
  - Forward secrecy.
- Mutual authentication.

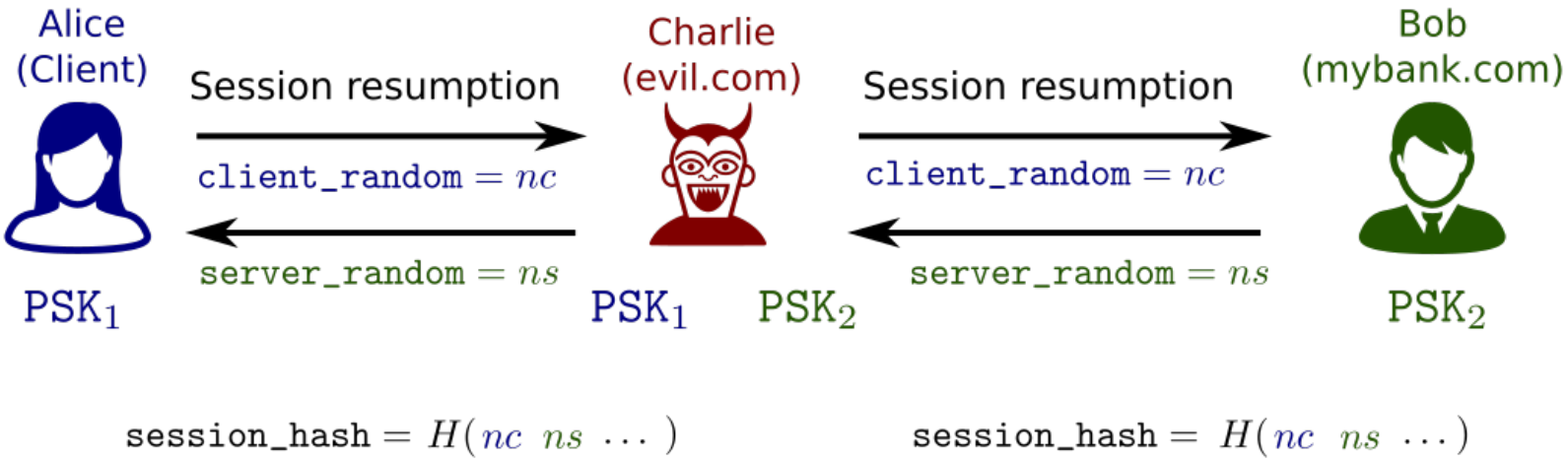
Attacking client authentication



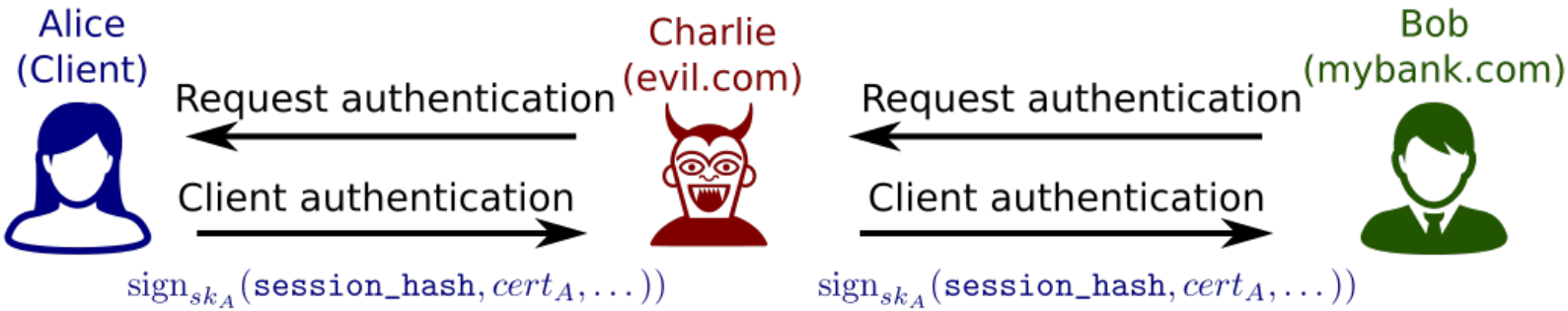
Attacking client authentication



Attacking client authentication



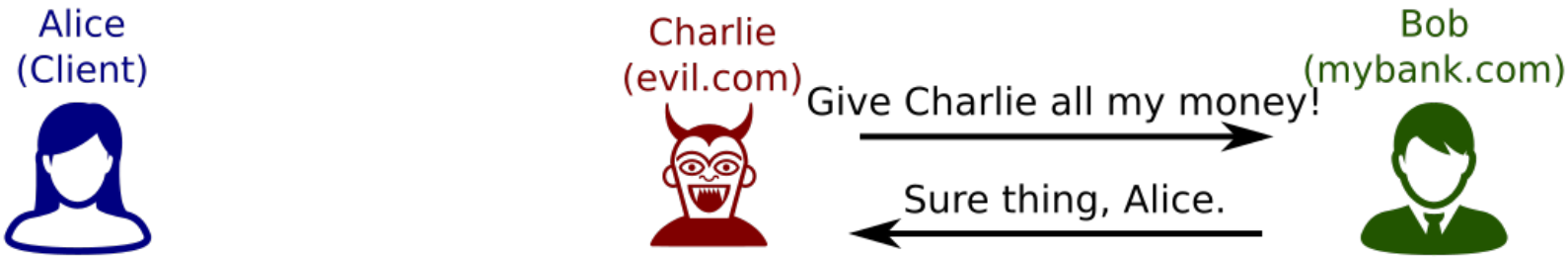
Attacking client authentication



$\texttt{session\_hash} = H(nc\ \ ns\ \ \ldots\ )$

$\texttt{session\_hash} = H(nc\ \ ns\ \ \ldots)$

Attacking client authentication



Conclusions

- This story has a happy ending: revision 10 was proved secure, and the changes in revision 11 appear to address the attack.
- First comprehensive analysis of the new TLS 1.3 modes and their interaction.
  - We confirmed the base design is solid.
  - Prevented a potential weakness.
- Our state machines and models provide insight into the structure of TLS implementations.
- Future work: improve and build upon this model.

Authors:

Cas Cremers
cas.cremers@cs.ox.ac.uk

Marko Horvat
marko.horvat@cs.ox.ac.uk

Sam Scott
sam.scott.2012@live.rhul.ac.uk

Thyla van der Merwe
thyla.vandermerwe.2012@live.rhul.ac.uk