Security of TLS ≤1.2

The ACCE model

TLS Crypto Seminar

February 7, 2019

Joseph Jaeger

UC San Diego

some slides & formatting stolen from Felix Günther

Today's Plan

UC San Diego

Goal

- What is the ACCE security model? Why was it needed for studying TLS?
- Dig into the details of the formalism.

Part I Background

- Stateful Length-Hiding Authenticated Encryption
- Authenticated Key Exchange

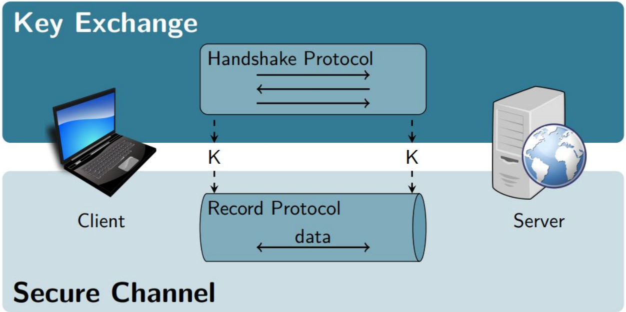
Part II ACCE Security Model

- Authenticated and Confidential Channel Establishment
- TLS 1.2 Security Results (Time Permitting)

Background

TLS Components

From the first lecture:



Security Typically Desired:

- Handshake Protocol = Authenticated Key Exchange
- Record Protocol = Stateful Length Hiding Authenticated Encryption

UC San Diego

Formalisms based on:

On the Security of TLS-DHE in the Standard Model[1]

Tibor Jager
Horst Görtz Institute for IT Security
Bochum, Germany
tibor.jager@rub.de

Florian Kohlar
Horst Görtz Institute for IT Security
Bochum, Germany
florian.kohlar@rub.de

Sven Schäge[2]
University College London
United Kingdom
s.schage@ucl.ac.uk

Jörg Schwenk
Horst Görtz Institute for IT Security
Bochum, Germany
joerg.schwenk@rub.de

sLHAE Definition

Syntax

- $K \leftarrow\$ \mathsf{SE.Kg}$
- $(\mathrm{st}_e, \mathrm{st}_d) \leftarrow \mathsf{SE.Init}$
- $(C, \mathrm{st}_e) \leftarrow\$ \mathsf{SE.Enc}(K, \ell, H, m, \mathrm{st}_e)\ //|C| = \ell$
- $(M, \mathrm{st}_d) \leftarrow\$ \mathsf{SE.Dec}(K, H, C, \mathrm{st}_d)$

sLHAE Definition

UC San Diego

Security

Game $\mathrm{G}^{\mathrm{ae}}_{\mathcal{A},\mathsf{SE}}$	$\textsc{Enc}(M_0, M_1, \ell, H)$	$\textsc{Dec}(C, H)$
$b \leftarrow\$ \{0,1\}$	$u \leftarrow u + 1$	$v \leftarrow v + 1$
$u \leftarrow v \leftarrow 0$	$(C^0, \mathrm{st}_e^0) \leftarrow\$ \mathsf{SE.Enc}(K, \ell, H, M_0, \mathrm{st}_e)$	If $b = 0)$ then return $\perp$
$K \leftarrow\$ \mathsf{SE.Kg}$	$(C^1, \mathrm{st}_e^1) \leftarrow\$ \mathsf{SE.Enc}(K, \ell, H, M_1, \mathrm{st}_e)$	$(M, \mathrm{st}_d) \leftarrow \mathsf{SE.Dec}(K, H, C, \mathrm{st}_d)$
$(\mathrm{st}_e, \mathrm{st}_d) \leftarrow \mathsf{SE.Init}$	If $C^0 = \perp$ or $C^1 = \perp$ then return $\perp$	If $v > u$ or $C \neq C_v$ then $\mathsf{oos} \leftarrow \mathsf{true}$
$b' \leftarrow\$ \mathcal{A}^{\textsc{Enc},\textsc{Dec}}$	$(C_u, \mathrm{st}_e) \leftarrow (C^b, \mathrm{st}_e^b)$	If not oos then return M
Return $b = b'$	Return C_u	Return $\perp$

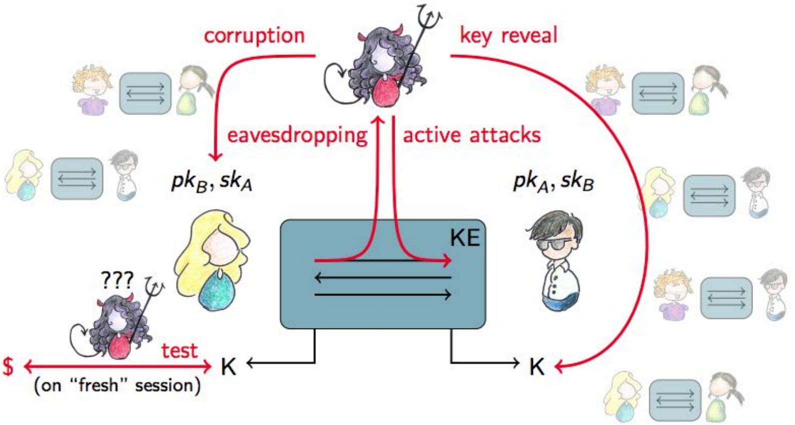
Security Typically Desired:

- All-in-one definition requiring left-right IND-CPA and INT-CTXT style security

Key Exchange Definition

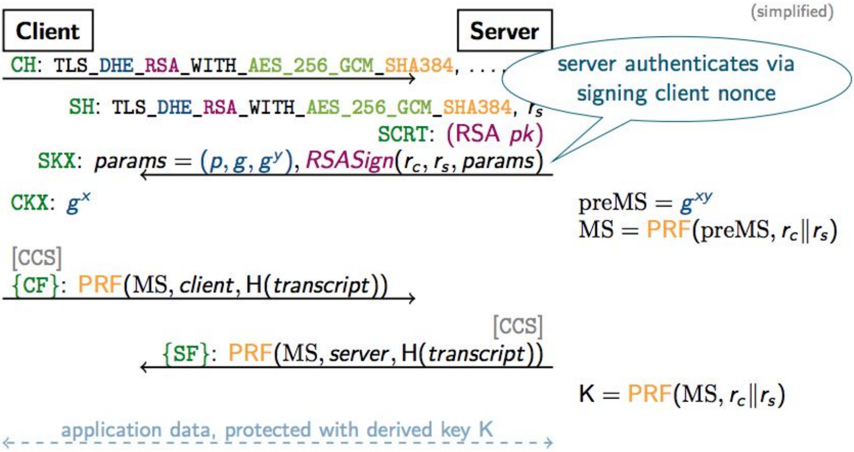
UC San Diego

Previously



TLS Example

UC San Diego



ACCE

ACCE

UC San Diego

Main Idea:

Squish encryption and key exchange security together into single notion.

Results

UC San Diego

On the Security of TLS-DHE in the Standard Model[1]

Tibor Jager
Horst Görtz Institute for IT Security
Bochum, Germany
tibor.jager@rub.de

Florian Kohlar
Horst Görtz Institute for IT Security
Bochum, Germany
florian.kohlar@rub.de

Sven Schäge[2]
University College London
United Kingdom
s.schage@ucl.ac.uk

Jörg Schwenk
Horst Görtz Institute for IT Security
Bochum, Germany
joerg.schwenk@rub.de

February 20, 2013

Main Result:

TLS-DHE is secure in this model

Results

UC San Diego

On the Security of the TLS Protocol: A Systematic Analysis*

Hugo Krawczyk, Kenneth G. Paterson**, and Hoeteck Wee***

Model:

Closely related to discussed ACCE model.
No client authentication.
No forward security.

Main Result:

TLS-RSA is secure in this model. (Under OW-PCA assumption.)
TLS-DH is secure in this model. (Under PRF-ODH assumption.)
TLS would be secure in this model with CCA secure encryption

Definition 1 (Matching conversations). *We say that* π_i^P *has a* matching conversation *with* $\pi_j^{P'}$ *if*

- *either* $P \in \mathcal{C}$ *and* $P' \in \mathcal{S}$, *or* $P \in \mathcal{S}$ *and* $P' \in \mathcal{C}$; *and*
- π_i^P *accepts; and*
- *the transcripts at both* π_i^P *and* $\pi_j^{P'}$ *begin with the same three messages* $(\text{CREQ}, \text{SRES}, \text{CRES})$.