On the Security of the Pre-Shared Key Ciphersuites of TLS

Yong Li [1], Sven Schäge[2], Zheng Yang[1],

Florian Kohlar[1], and Jörg Schwenk[1]

[1] Horst Görtz Institute for IT Security, Bochum
[2] University College London

Buenos Aires, Argentina
March 28, 2014

Outline

- Motivation
- Introduction to SSL/TLS and Pre-Shared Key Ciphersuites
- Security Analysis of Pre-Shared Key Ciphersuites of TLS
  - A Security Model for Authentication via (**Symmetric**) Pre-Shared Keys
  - Security Results for Pre-Shared Key Ciphersuites of TLS
- Summary

Outline

- **Motivation**
- Introduction to SSL/TLS and Pre-Shared Key Ciphersuites
- Security Analysis of Pre-Shared Key Ciphersuites of TLS
  – A Security Model for Authentication via (**Symmetric**) Pre-Shared Keys
  – Security Results for Pre-Shared Key Ciphersuites of TLS
- Summary

PSK-Ciphersuites of TLS

- TLS-PSK: Authentication with Symmetric Keys (PSKs)

- Authentication of resource-restricted clients like smart-cards, SIM Cards, ID Cards, ...

PSK-Ciphersuites of TLS

- Several interesting and important scenarios for TLS with pre-shared keys:
  - Authentication protocol based on TLS-PSK for **EMV smart cards**
  - Application of TLS-PSK in the **Generic Authentication**, the **3GGP mobile phone** standard for UMTS and LTE
  - New electronic **German ID** (eID) card supports online remote authentication

Outline

- Motivation
- **Introduction to SSL/TLS and Pre-Shared Key Ciphersuites**
- Security Analysis of Pre-Shared Key Ciphersuites of TLS
  - A Security Model for Authentication via (**Symmetric**) Pre-Shared Keys
  - Security Results for Pre-Shared Key Ciphersuites of TLS
- Summary

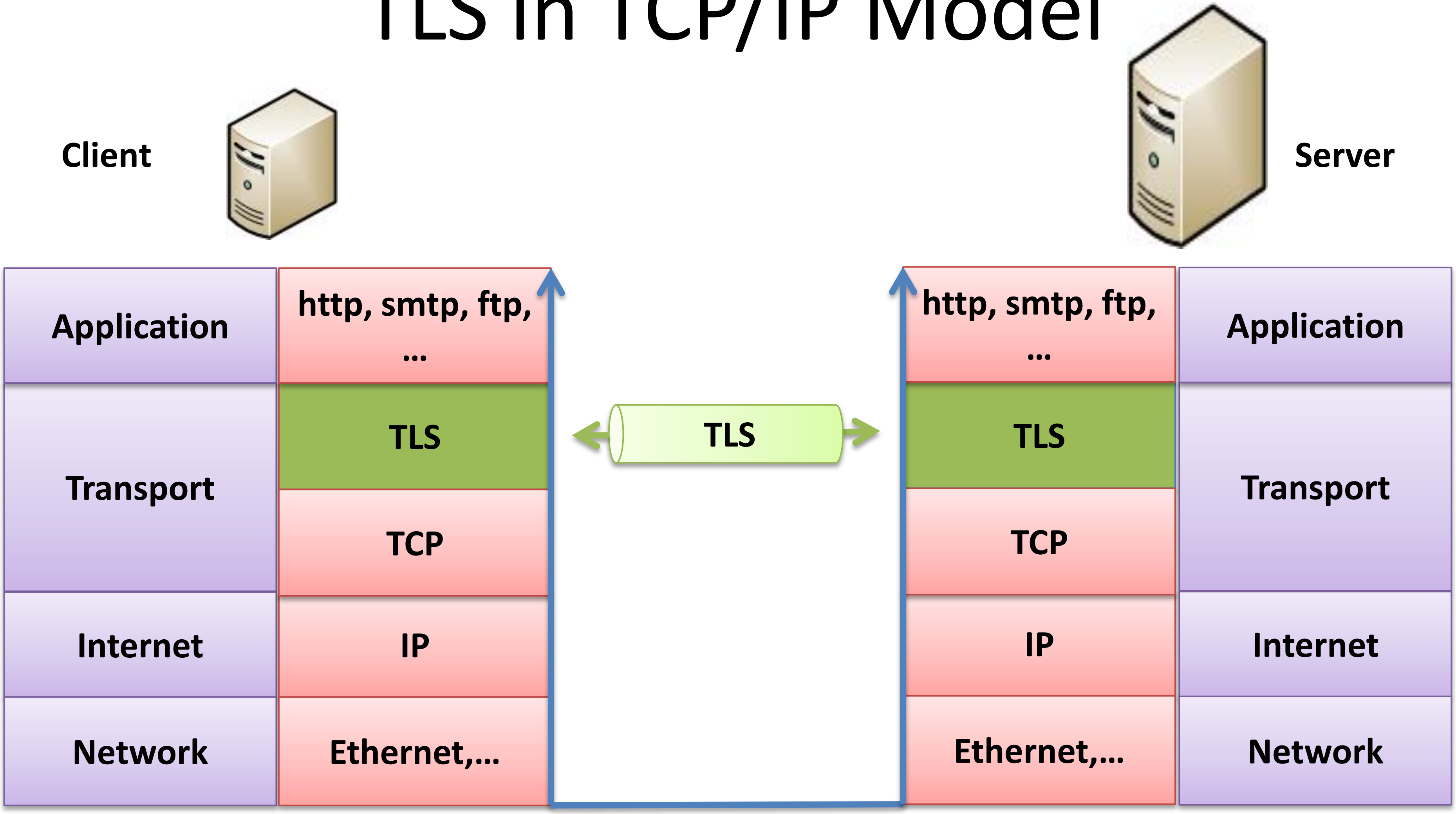
What is TLS?

- **T**ransport **L**ayer **S**ecurity

- **C**ryptographic **p**rotocols which provide secure communication over the **I**nternet

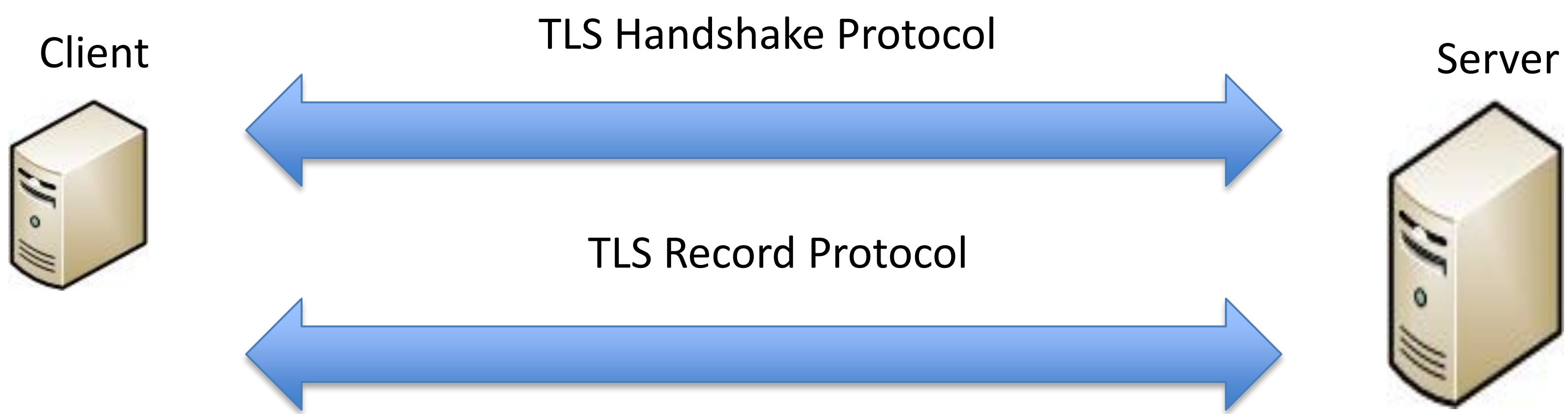
- Confidentiality, Integrity and Authenticity

TLS in TCP/IP Model



Secure Communication Channel

TLS Sessions: Handshake + Record Layer



TLS Handshake:

- **cryptographic parameters**
- **authentication**
- **session key k**

TLS Record Layer:

- Data **encryption** and **authentication** using **the session key k**

Pre-Shared Key Ciphersuites of TLS

3 families of Pre-Shared Key Ciphersuites of TLS:

- Pre-shared Keys (**TLS_PSK**): Session key is solely based on the secret pre-shared keys (**PSK**).
- RSA Encryption (**TLS_RSA_PSK**): Session key is dependent on **PSK** and a freshly exchanged **secret** via **RSA** Encryption.
- Diffie-Hellman key exchange (**TLS_DHE_PSK**): Session key is dependent on **PSK** and **Diffie-Hellman** key exchange.

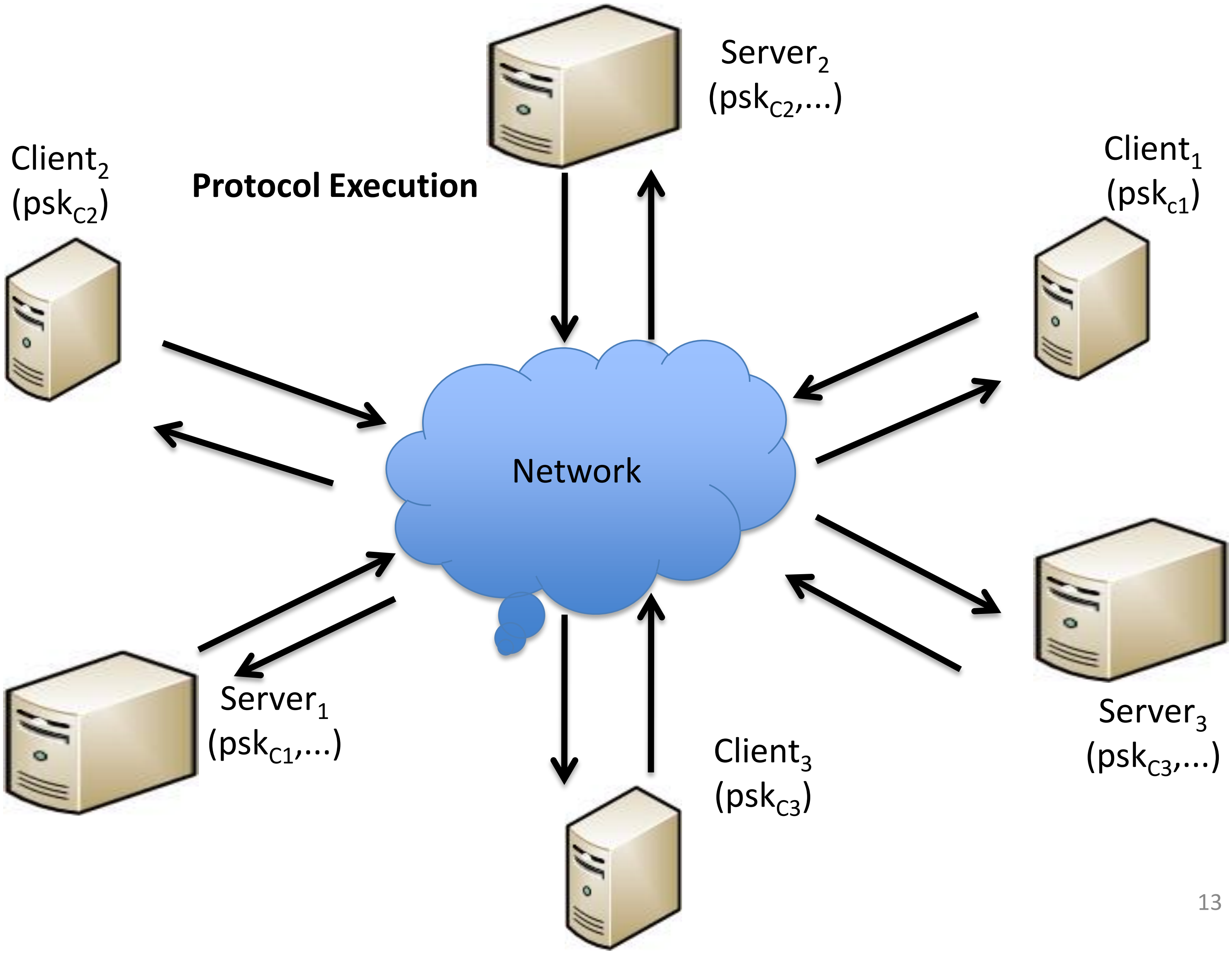
Outline

- Motivation
- Introduction to SSL/TLS and Pre-Shared Key Ciphersuites
- **Security Analysis of Pre-Shared Key Ciphersuites of TLS**
  - **A Security Model for Authentication via (Symmetric) Pre-Shared Keys**
  - Security Results for Pre-Shared Key Ciphersuites of TLS
- Summary

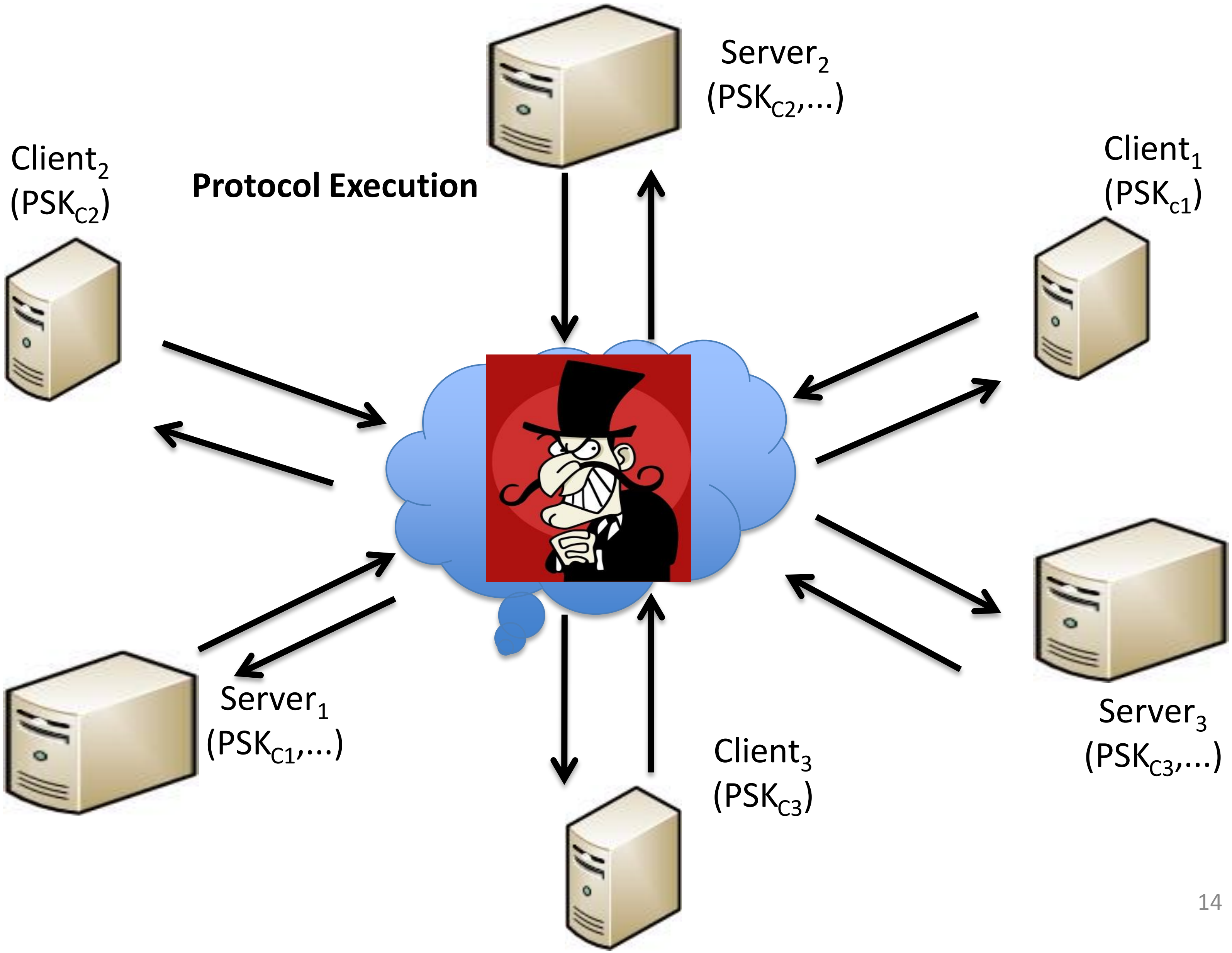
ACCE Model for PSK- Ciphersuites of TLS

- Simple extension of the **A**uthenticated and **C**onfidential **C**hannel **E**stablishment (**ACCE**) model [JKSS'2012] :
  - Cover scenarios **with pre-shared, symmetric keys**
- Model described by Two components
  - **Security Model**
  - **Security Definition**

Real World without adversary (1)



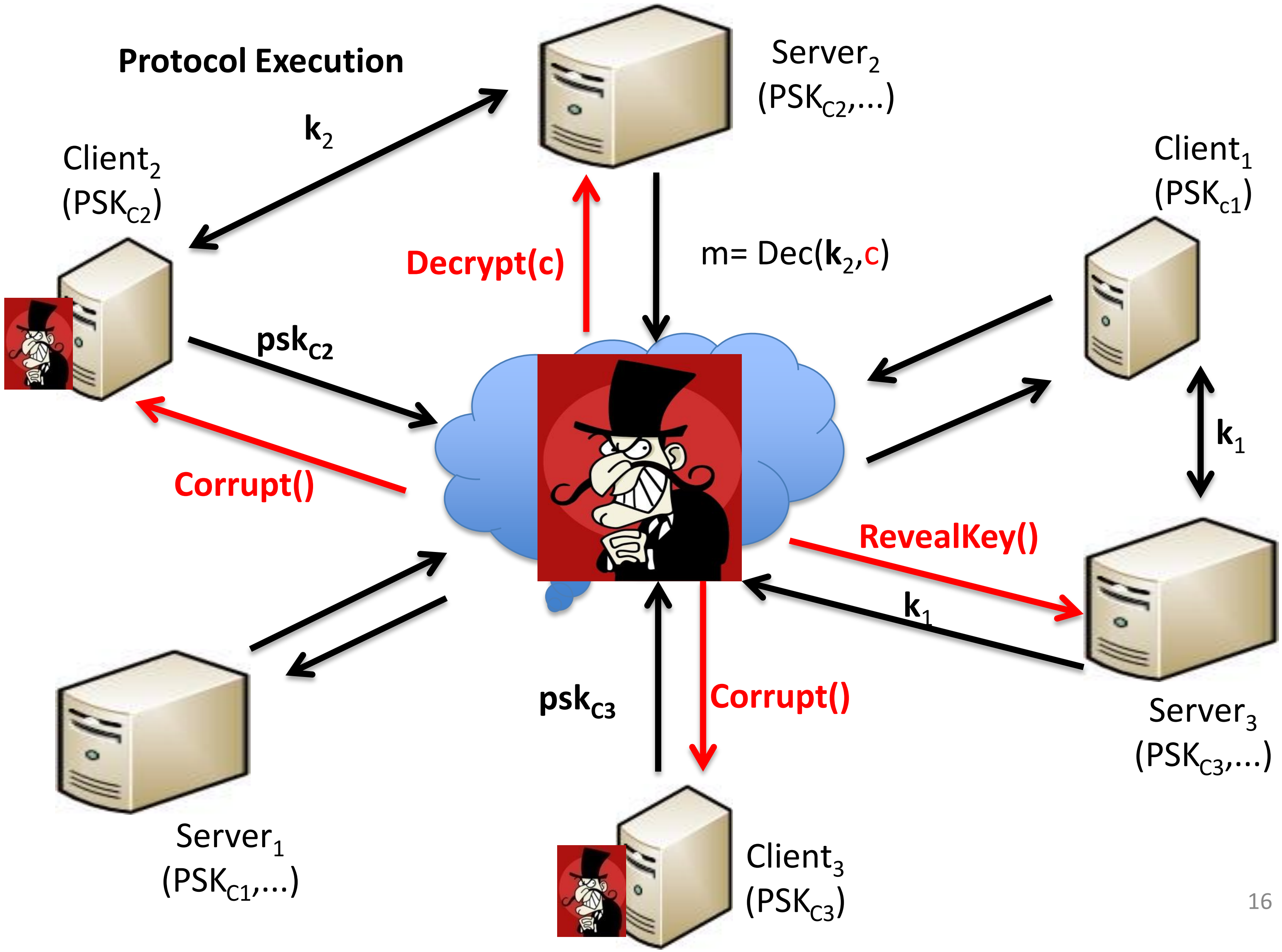
Real World with adversary (2)



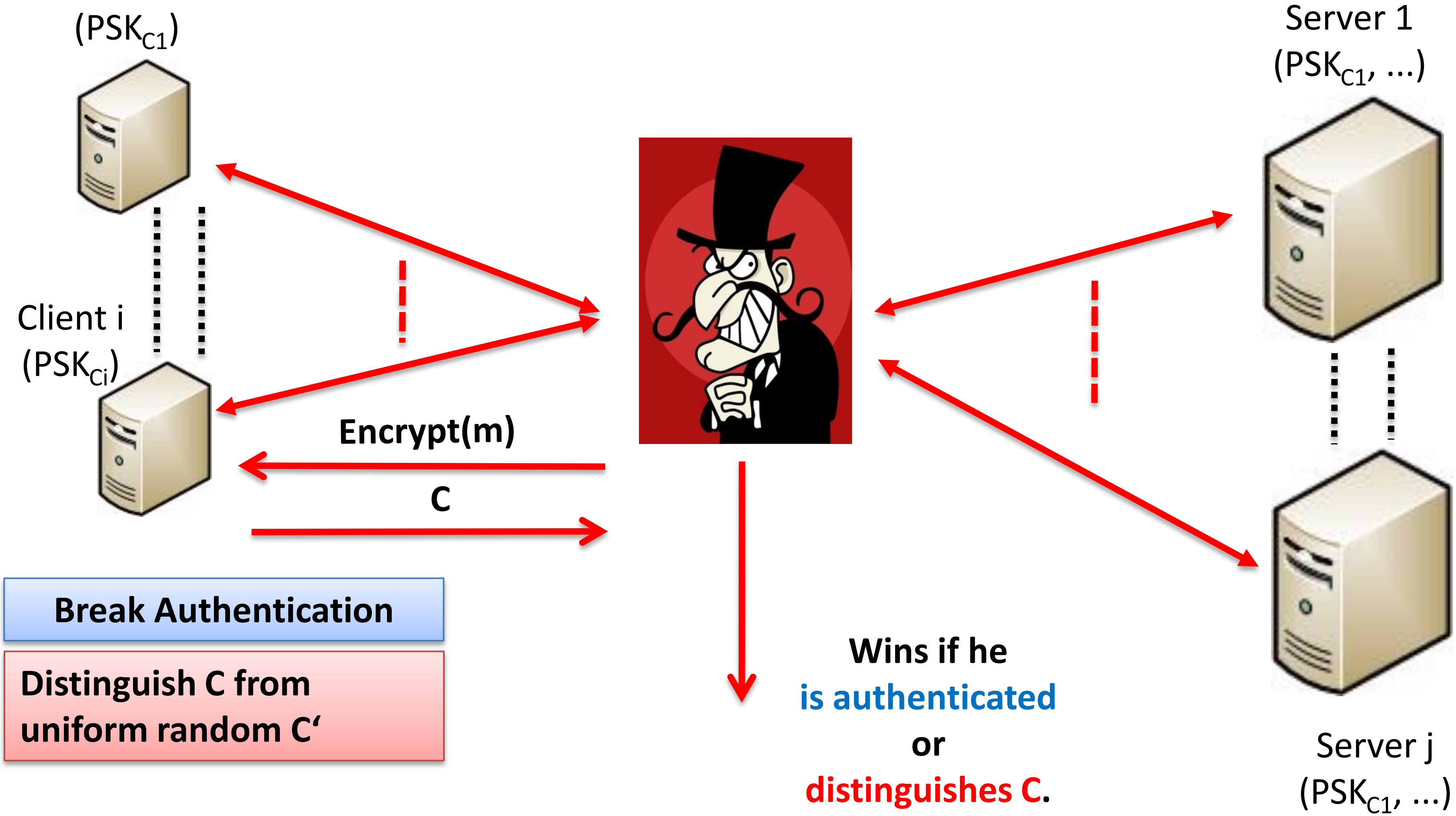
ACCE Adversary Model (1)

- An adversary is allowed to send the following queries to the honest parties:
  - **Send**()
  - **RevealKey**()
  - **Corrupt**()
  - **Encrypt**()
  - **Decrypt**()

Real World without adversary (2)



ACCE Security Definition (1)



ACCE Security Definition (2)

The adversary breaks the protocol if

- he is successfully authenticated by a Server (or Client) (**Authentication Property**) or

- distinguishes **C** from random (**Ciphertext Indistinguishability**).
  - with **Perfect Forward Secrecy**:
    - retain **Ciphertext Indistinguishability** for protocol sessions even if the long-term secrets of the **client** und **server** are exposed **after** session key is created.
  - with **asymmetric** Perfect Forward Secrecy:
    - similar to that of classical perfect forward secrecy except that **only the client** is allowed to be corrupted

Outline

- Motivation
- Introduction to SSL/TLS and Pre-Shared Key Ciphersuites
- **Security Analysis of Pre-Shared Key Ciphersuites of TLS**
  - A Security Model for Authentication via (**Symmetric**) Pre-Shared Keys
  - **Security Results for Pre-Shared Key Ciphersuites of TLS**
- Summary

TLS_PSK Handshake

Client has PSK

|PSK|=N bytes long

Server has PSK

|PSK|=N bytes long

Cipher Suite Agreement Phase:

r_C, Supported Cipher Suites →

← r_S, selected Cipher Suite

Key Exchange Phase:

PSK identity pointing to the PSK used for authentication ↔

Client:

pms=N||0...0||N||PSK

ms = PRF(pms; Label$_1$, r_C, r_S)

k = PRF(ms; Label$_2$, r_C, r_S)

Server:

pms=N||0...0||N||PSK

ms = PRF(pms; Label$_1$, r_C, r_S)

k = PRF(ms; Label$_2$, r_C, r_S)

Symmetric Encryption Phase:

fin_C = PRF(ms; Label$_3$, H(prev. data))

Enc(**k**; $const_S$, fin_C) →

"Accept", session key k with Client

← Enc(**k**; $const_C$, fin_S)

fin_S = PRF(ms; Label$_4$,H(prev. data))

"Accept", session key k with Server

TLS-PSK is a Secure ACCE Protocol

Theorem:

TLS-PSK is a secure ACCE protocol **without forward secrecy**, if

- the PRF is a **secure pseudo-random function**,
- hash function H is **secure collision-resistant hash function**,
- The symmetric encryption is **sLHAE-secure**.

sLHAE [PRS'11]:

- Definition for **symmetric ciphers**
- Exactly for **TLS Protocol**

$$\epsilon_{\mathsf{tls}} \leq \epsilon_{\mathsf{auth}} + \epsilon_{\mathsf{enc}}$$

$$= (d\ell)^2 \left(\frac{1}{2^{\lambda-1}} + 6 \cdot \epsilon_{\mathsf{PRF}} + 2 \cdot \epsilon_{\mathsf{H}} + \frac{1}{2^{\mu-1}} + 6 \cdot \epsilon_{\mathsf{StE}} \right)$$

Double Pseudo-Random Functions (**DPRF**)

- **DPRF**: a class of **PRF** with two input-keys
- The **output** of the **DPRF** is **indistinguishable from random** even if the adversary chooses one key which will be revealed

- A **DPRF** is easy to construct:

$$\mathbf{DPRF(k1; k2; m) := PRF1(k1; m) \oplus PRF2(k2; m)}$$

TLS_DHE_PSK Handshake

Client has PSK

$|PSK| = N$ bytes long

Server has PSK

$|PSK| = N$ bytes long

Cipher Suite Agreement Phase:

r_C, Supported Cipher Suites →

← r_S, selected Cipher Suite

Key Exchange Phase:

Server:

$c \leftarrow Z_q$

$T = g^{cs} \bmod p$

$|T| = L_T$ bytes long

pms := $L_T || T || N || PSK$

ms = DPRF(pms;$Label_1$,r_C,r_S)

k = PRF(ms;$Label_2$,r_C,r_S)

← $g^s \bmod p$

$g^c \bmod p$ →

Client:

$c \leftarrow Z_q$

$T = g^{sc} \bmod p$

$|T| = L_T$ bytes long

pms := $L_T || T || N || PSK$

ms = DPRF(pms;$Label_1$,r_C,r_S)

k = PRF(ms;$Label_2$,r_C,r_S)

Symmetric Encryption Phase:

fin_S = PRF(ms; $Label_3$, H(prev. data))

← Enc(**k**; $const_S$, fin_S)

"Accept", session key k with Server

fin_C = PRF(ms; $Label_4$, H(prev. data))

Enc(**k**; $const_C$, fin_C) →

"Accept", session key k with Client

Double Pseudo-Random Functions (DPRF)

- In order to prove perfect forward secrecy in TLS_**DHE**_PSK, we assume that
  - TLS-PRF constitutes a secure DPRF
  - The key space of the DPRF:
    - $\mathbf{K}_{\mathbf{DPRF1}}$: the key space of the pre-shared key **PSK**
    - $\mathbf{K}_{\mathbf{DPRF2}}$ **:** the key space of the freshly generated **Diffie-Hellman** secret **T**

Example: Implementation in TLS1.1:

PRF(PSK,T; m) = HMAC_MD5'(T; m) $\oplus$ **HMAC_SHA'(PSK; m)**

TLS-DHE-PSK is a Secure ACCE Protocol

__Theorem:__

TLS-DHE-PSK is a secure ACCE protocol **with perfect forward secrecy**, if

- **DPRF$_{\text{TLS}}$** is a **double secure pseudo-random function,**
- **PRF$_{\text{TLS}}$** is a **secure pseudo-random function (PRF)**,
- hash function H is **secure collision-resistant hash function**,
- the **DDH assumption** holds in the Diffie-Hellman group,
- the symmetric encryption is **sLHAE-secure**.

$$\epsilon_{\mathsf{tls}} \leq (d\ell)^2 \left(\frac{1}{2^{\lambda-1}} + 3 \cdot \epsilon_{\mathsf{DPRF}} + 3 \cdot \epsilon_{\mathsf{PRF}} + 2 \cdot \epsilon_{\mathsf{H}} + \frac{1}{2^{\mu-1}} + \epsilon_{\mathsf{DDH}} + 6 \cdot \epsilon_{\mathsf{StE}} \right)$$

TLS_RSA_PSK Handshake

Client has PSK

$|PSK| = N$ bytes long

Server has PSK and RSA key pair: (pk_S, sk_S)

$|PSK| = N$ bytes long

Cipher Suite Agreement Phase:

r_C, Supported Cipher Suites →

← r_S, selected Cipher Suite

Key Exchange Phase:

Client:

random value R

$C = Enc(pk_S, R)$

$|R| = 46$ bytes long

V = 2-byte version number

$pms := 48||V||R||N||PSK$

$ms = DPRF(pms; Label_1, r_C, r_S)$

$k = PRF(ms; Label_2, r_C, r_S)$

Ciphertext: C →

Server:

random value R

$R = Dec(sk_S, R)$

$|R| = 46$ bytes long

V = 2-byte version number

$pms := 48||V||R||N||PSK$

$ms = DPRF(pms; Label_1, r_C, r_S)$

$k = PRF(ms; Label_2, r_C, r_S)$

Symmetric Encryption Phase:

← $Enc(\mathbf{k}; const_S, fin_S)$

$fin_S = PRF(ms; Label_3, H(prev. data))$

"Accept", session key k with Server

$Enc(\mathbf{k}; const_C, fin_C)$ →

$fin_C = PRF(ms; Label_4, H(prev. data))$

"Accept", session key k with Client

26

TLS-RSA-PSK is a Secure ACCE Protocol

<u>**Theorem:**</u>

TLS-RSA-PSK is a secure ACCE protocol **with asymmetric perfect forward secrecy**, if

- the **PRF$_{\text{TLS}}$** is a **secure pseudo-random function (PRF)** when keyed with the **master** secret
- the **PRF$_{\text{TLS}}$** is a **secure double pseudo-random function (DPRF)** when keyed with the **pre-master** secret
- hash function H is **secure collision-resistant hash function,**
- the PKE scheme is **IND-CCA secure**
- the record layer cipher is **secure (sLHAE)**

$$\epsilon_{\mathsf{tls}} \leq (d\ell)^2 \left(\frac{1}{2^{\lambda-1}} + \epsilon_{\mathsf{PKE}} + 3 \cdot \epsilon_{\mathsf{DPRF}} + 3 \cdot \epsilon_{\mathsf{PRF}} + 2 \cdot \epsilon_{\mathsf{H}} + \frac{1}{2^{\mu-1}} + 6 \cdot \epsilon_{\mathsf{StE}} \right)$$

Outline

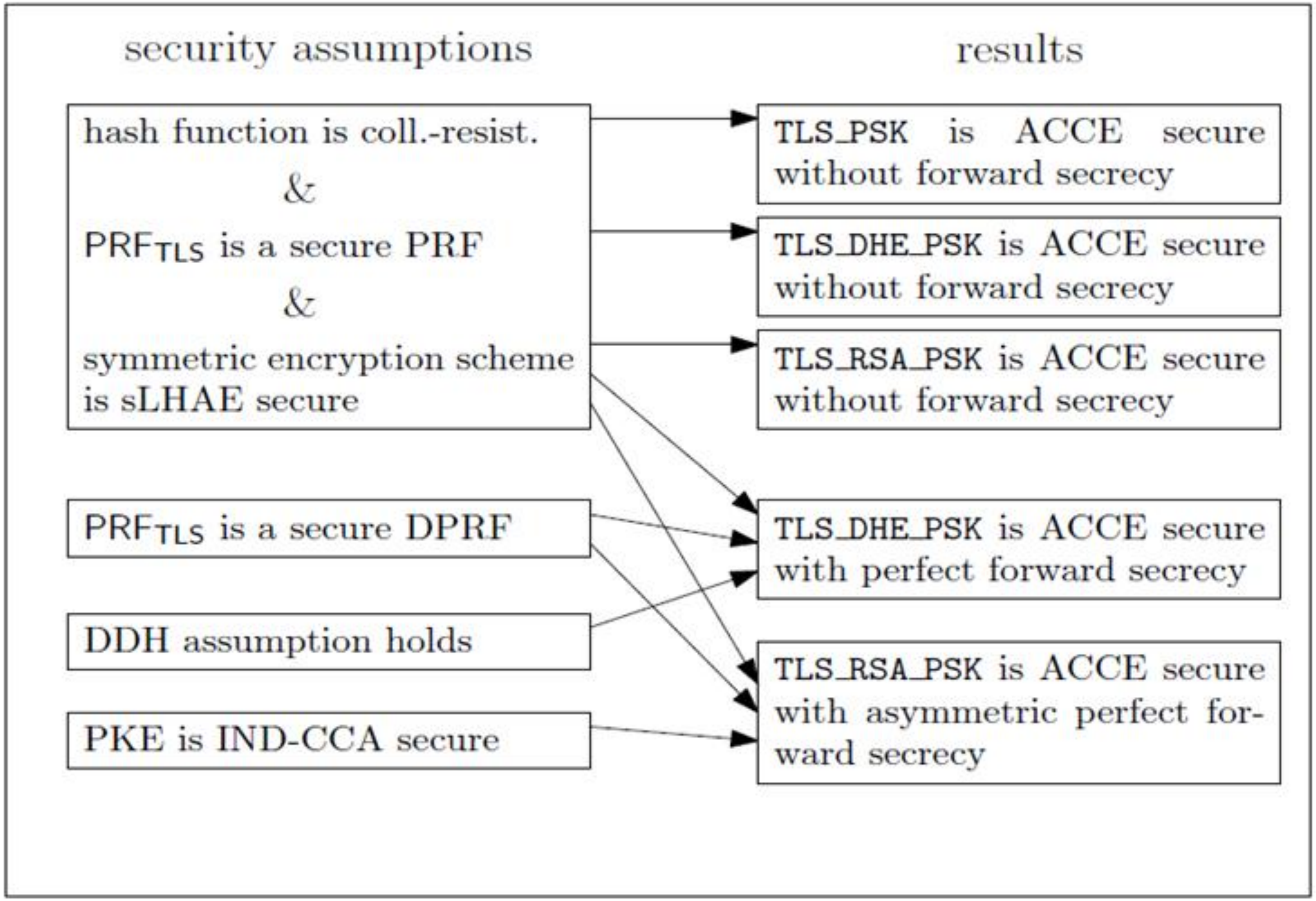
- Motivation
- Introduction to SSL/TLS and Pre-Shared Key Ciphersuites
- Security Analysis of Pre-Shared Key Ciphersuites of TLS
  - A Security Model for Authentication via (**Symmetric**) Pre-Shared Keys
  - Security Results for Pre-Shared Key Ciphersuites of TLS
- **Summary**

Summary

- An extension of the **ACCE** model [JKSS'2012] for authentication via (**symmetric**) pre-shared keys
  - without **forward secrecy**,
  - with **asymmetric perfect secrecy** and
  - with **perfect forward secrecy**.

- Provide a security analysis of **all three TLS-PSK ciphersuites** in standard model.

Summary


security assumptions
results
hash function is coll.-resist.
&
PRF$_{\mathsf{TLS}}$ is a secure PRF
&
symmetric encryption scheme is sLHAE secure
PRF$_{\mathsf{TLS}}$ is a secure DPRF
DDH assumption holds
PKE is IND-CCA secure
TLS_PSK is ACCE secure without forward secrecy
TLS_DHE_PSK is ACCE secure without forward secrecy
TLS_RSA_PSK is ACCE secure without forward secrecy
TLS_DHE_PSK is ACCE secure with perfect forward secrecy
TLS_RSA_PSK is ACCE secure with asymmetric perfect forward secrecy