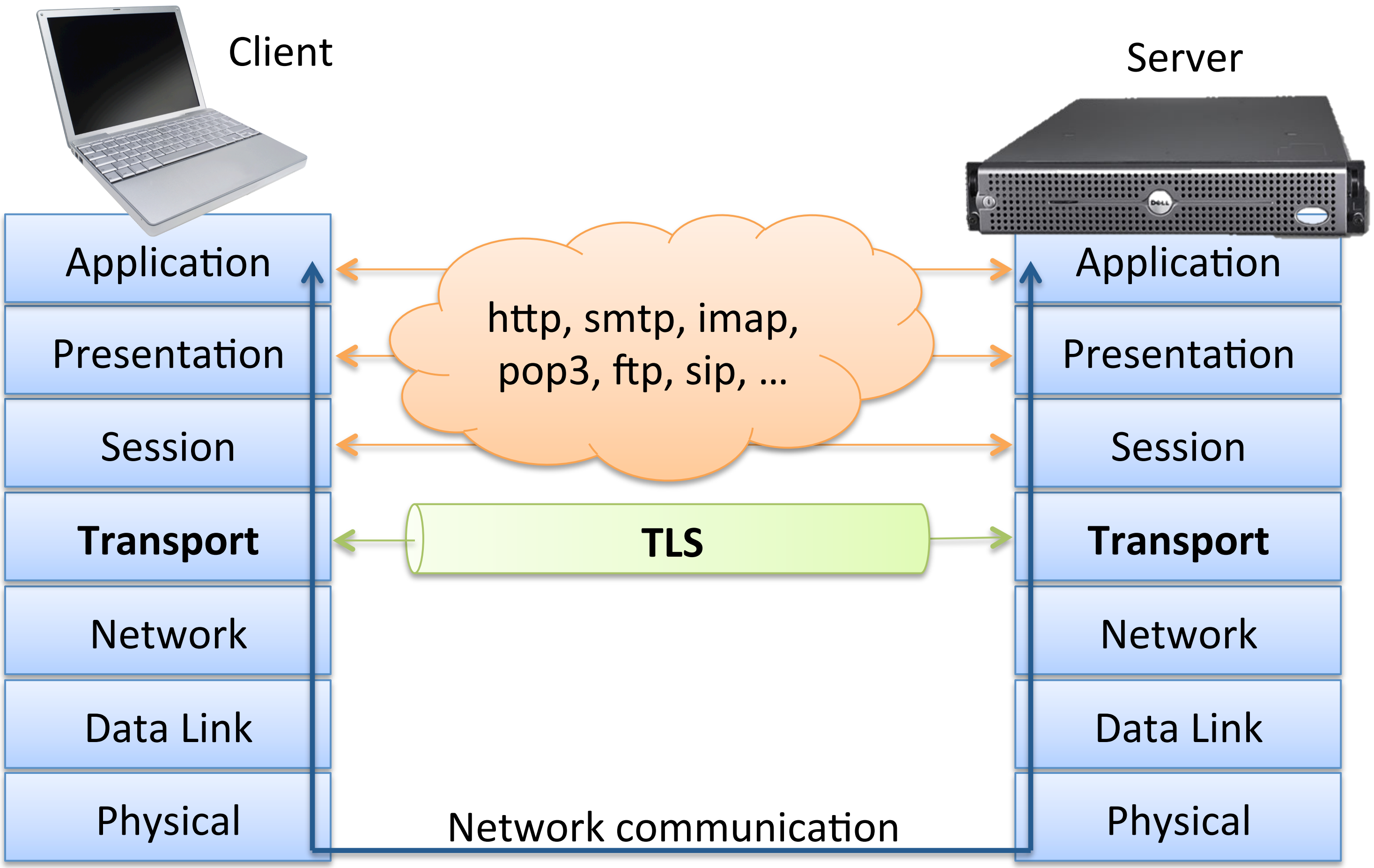
A Standard-Model Security Analysis of TLS-DHE

Tibor Jager[1], Florian Kohlar[2], Sven Schäge[3], and Jörg Schwenk[2]

[1] Karlsruhe Institute of Technology
[2] Horst Görtz Institute for IT Security, Bochum
[3] University College London

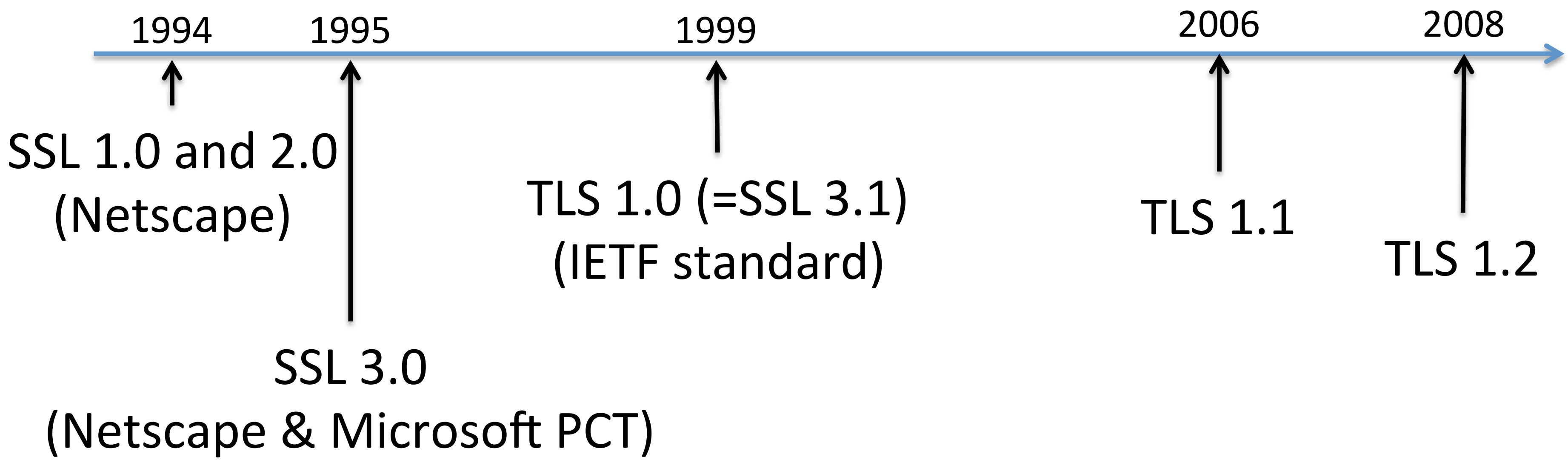
CRYPTO 2012

Transport Layer Security (TLS)



Goal: provide **confidential** and **authenticated** communication channel

TLS and SSL



- TLS 1.0 and 1.1 still widely used
- In this talk: TLS ≈ TLS 1.0 ≈ TLS 1.1 ≈ TLS 1.2

TLS Sessions:
Handshake + Record Layer

Handshake:

- Negotiation of **cryptographic parameters** (selection of *Cipher Suite*)
- **Authentication**
- Establishment of **session key** k

Record Layer:

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

Cipher Suites

- Standardized **selection of algorithms** for key exchange, signature, encryption, hashing
  - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- **3 groups** of Cipher Suites:
  - Ephemeral Diffie-Hellman (TLS-DHE)
  - Static Diffie-Hellman (TLS-DH)
  - RSA encryption (TLS-RSA)
- Handshake protocol is (slightly) different for each group

The Cryptographic Core of TLS-DHE Handshake

C has signature key (pk_C, sk_C)

S has signature key (pk_S, sk_S)

1. Cipher suite agreement:

C → S: r_C, supported Cipher Suites

S → C: r_S, selected Cipher Suite

2. Key exchange:

C: $c \leftarrow Z_q$

S: $s \leftarrow Z_q$

S → C: g^s, Sig(sk_S; g^s, *some previous data*)

C → S: g^c, Sig(sk_C; g^c, *some previous data*)

C:
$pms = g^{cs}$
$ms = PRF(pms; L_1, r_C, r_S)$
$k = PRF(ms; L_2, r_C, r_S)$

S:
$pms = g^{cs}$
$ms = PRF(pms; L_1, r_C, r_S)$
$k = PRF(ms; L_2, r_C, r_S)$

3. FINISHED messages:

S: $fin_S = PRF(ms; L_3,$ *prev. data*$)$

S → C: $Enc(k; const_S, fin_S)$

C: "Accept" key k with partner S

C: $fin_C = PRF(ms; L_4,$ *prev. data*$)$

C → S: $Enc(k; const_C, fin_C)$

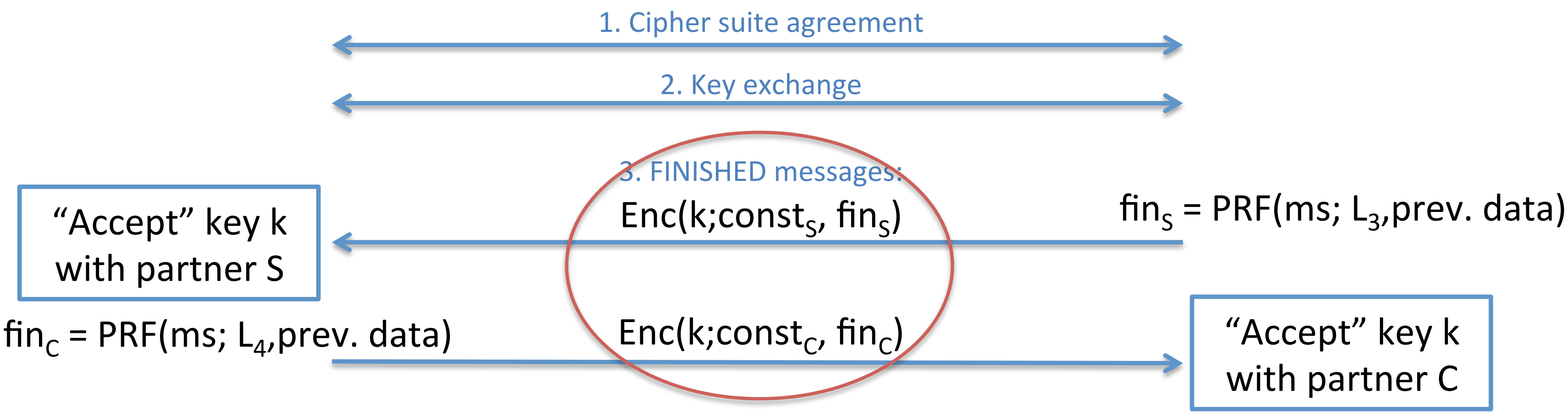
S: "Accept" key k with partner C

Is this **secure**?

Secure Authenticated Key Exchange

- Secure AKE guarantees:
  - **Authentication** of communication partners
  - **Good cryptographic keys**
    - "Real" key should be **indistinguishable** from random value
- **Several security models** formalizing AKE security
  - [BR'93, BJM'99, CK'01, LLM`07, …]
  - We use an enhanced version of Bellare-Rogaway
    - Adopted to **public-key setting**
    - Adversary can **forward, alter, drop, replay, …** any message
    - Adaptive **corruptions**, **perfect forward secrecy**, security against **key-compromise impersonation**

The TLS Handshake is not a Provably Secure AKE Protocol

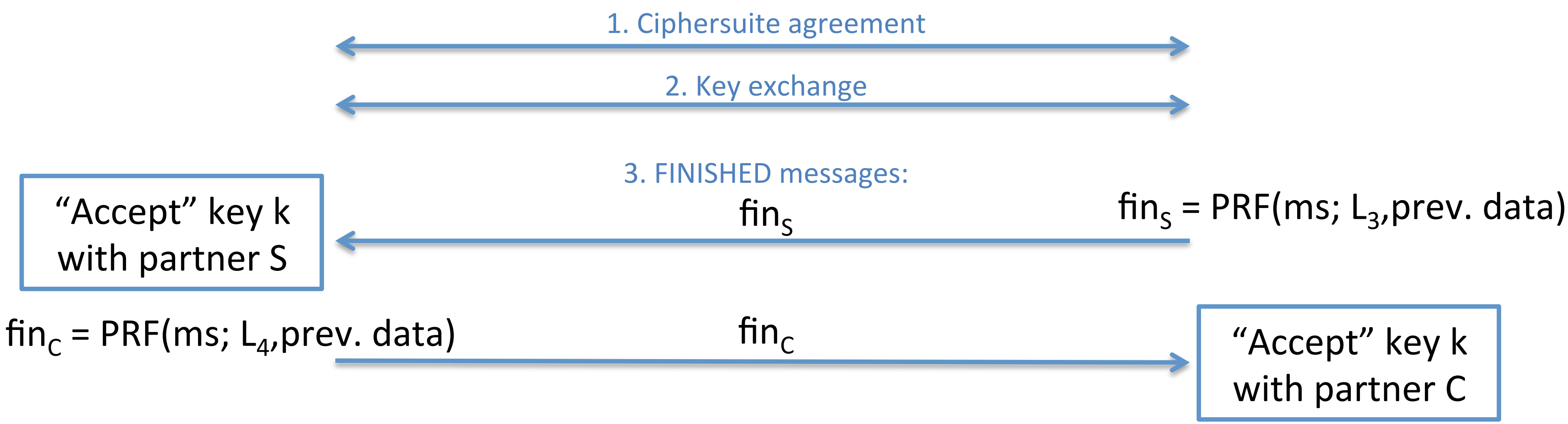


- $Enc(k;const_S,fin_S)$ **allows to distinguish** real key k from random
  - Applies to TLS-DHE, TLS-DHS, and TLS-RSA

Unsatisfying Situation

- TLS is the **most important** security protocol in practice
- TLS Handshake **is insecure** in **any** AKE security model based on key-indistinguishability
- **Two approaches** to resolve this issue:
  1. Consider "truncated" TLS Handshake [MSW'10], **without encryption** of FINISHED messages
  2. Develop a **new security model**

1^{st} Approach: "Truncated TLS"



Theorem:

Truncated **TLS-DHE** Handshake is a secure AKE protocol, if

- the PRF is a **secure pseudo-random function,**
- the digital signature scheme is **EUF-CMA secure,**
- the **DDH assumption** holds, and
- the **PRF-ODH assumption** holds

Comparison to Previous Work

Truncated TLS: Morissey, Smart, Warinschi '10

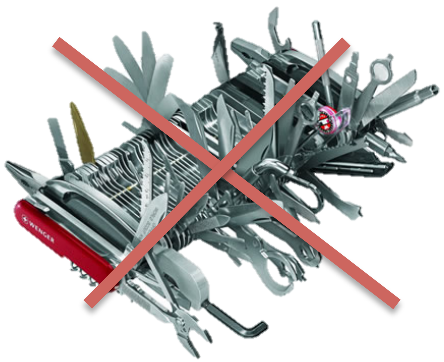
Morrissey, Smart, Warinschi '10	Our work
Bellare-Rogaway Model	Bellare-Rogaway Model
TLS_DHE, TLS_DH, TLS_RSA[1]	TLS_DHE
Random Oracle Model	Standard Model[2]

[1] Assumes different RSA encryption scheme
[2] Requires PRF-ODH assumption

Both results do **not** consider the **real TLS Handshake**…!

2nd Approach: New Security Model

- Secure AKE provides **indistinguishable keys**
  - Key can be used in **any further application**
  - **Too strong** for TLS Handshake
  - **Stronger than necessary**: TLS uses keys for **Record Layer**
- Can we describe a **new security model** which is
  - **strong enough** to provide security, but
  - **weak enough** to be achievable by TLS?



but

Authenticated Confidential Channel Establishment (ACCE)

- Simple extension of the AKE model:
  - Explicit **authentication** of communication partners
  - ~~**Good cryptographic keys**~~
    Authenticated and **confidential** channel
- ACCE considers **Handshake + Record Layer**
  - Requires that
    - Encryptions are **indistinguishable**
    - Ciphertexts are **authentic**

TLS-DHE is a Secure ACCE Protocol

Theorem:

TLS-DHE is a secure ACCE protocol, if

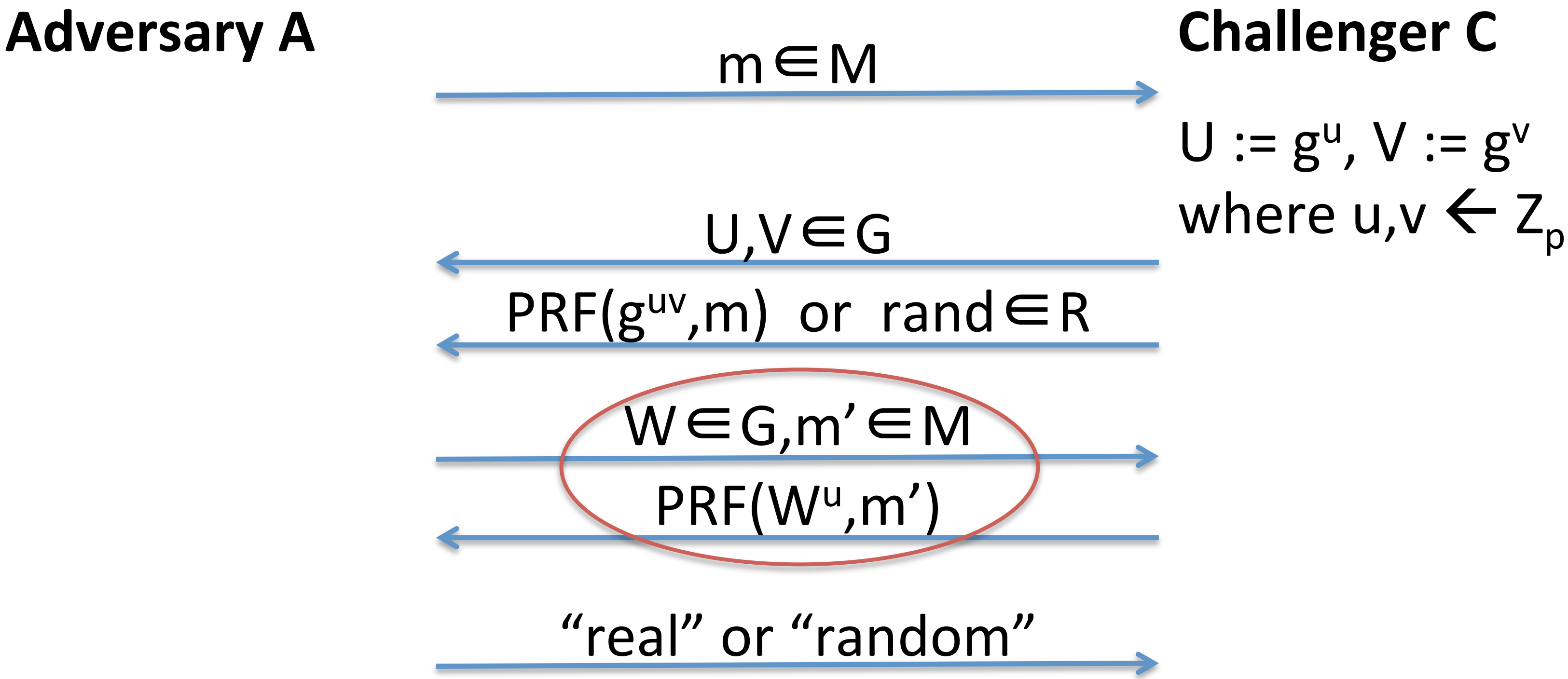
- the PRF is a **secure pseudo-random function**,
- the digital signature scheme is **EUF-CMA secure**,
- the **DDH assumption** holds in the Diffie-Hellman group,
- the **PRF-ODH assumption** holds, and
- the **Record Layer cipher is secure** (sLHAE)

Stateful Length-Hiding Authenticated Encryption [PRS'11]:

- Security notion for symmetric ciphers
- Captures exactly what is **expected from TLS Record Layer**
- **Achieved by CBC-based ciphersuites** in TLS 1.1 and 1.2

The PRF-ODH Assumption

- Let G = <g> be a group with order p,
  let PRF : G x M → R be a function



- **PRF-ODH assumption**: no efficient attacker can distinguish $PRF(g^{uv},m)$ from random
  - Variant of **Oracle Diffie-Hellman** assumption [ABR'01]

Is PRF-ODH *really* necessary?

- Not if
  - **no corruptions of long-term secrets** are allowed, or
  - **small changes** are made to TLS-DHE Handshake
    - E.g. making it more similar to Σ_0 [CK'02]
- **Impossible** to avoid, if
  - security model **with corruptions** is considered, and
  - reduction uses **attacker and PRF** as **black-box**

Summary and Open Problems

- AKE-security proof for **Truncated TLS-DHE Handshake**
- New **ACCE security** model
  – Alternative approach: “Relaxed yet composable security notions for key exchange” [BFSWW`12]
- ACCE-security proof for **TLS-DHE** with suitable Record Layer
- Many open problems
  – TLS is much more complex - we considered only the **cryptographic core** of TLS-DHE
  – Similar analysis of **TLS-DH** and **TLS-RSA** possible?