Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer

Christian Badertscher\textsuperscript{1}, Christian Matt\textsuperscript{1}, Ueli Maurer\textsuperscript{1}, Phil Rogaway\textsuperscript{2}, Björn Tackmann\textsuperscript{3}

\textsuperscript{1}ETH Zurich, \textsuperscript{2}UC Davis, \textsuperscript{3}UC San Diego
The Handshake of TLS 1.3
The Handshake of TLS 1.3

Ideal abstraction of the handshake [DFG15, KMO14]: A shared key resource
The Record Layer of TLS 1.3
The Record Layer of TLS 1.3

TLS 1.3 Type 23
Associated Data

Record Payload Protection

Insecure Channel

Record Payload Protection

Fragment and Associated Data

TLS 1.3 Type 23
The Record Layer of TLS 1.3

Structure of transmitted packets:
• Non-private header
• Private payload
• Both parts are authentic
The Record Layer of TLS 1.3

Associated Data

Fragment

Enc

Insecure Channel

Record Payload Protection

Fragment and Associated Data

TLS 1.3 Type 23

Internal values

TLS 1.3 Type 23

Enc
Authenticated Encryption with Associated Data

Key

Associated Data

Nonce

Plaintext

Enc

Deterministic Encryption Algorithm

Ciphertext
Authenticated Encryption with Associated Data

Key

Associated Data

Nonce

Ciphertext

Deteministic Decryption Algorithm

Plaintext

or
AEAD Security Game

See [HKR15]
AEAD Security Game

\[
\text{Enc, } \text{AD}, \text{, }, \text{,} \quad \text{Dec, } \text{AD}, \text{, }, \text{,}
\]

Real

\[
\text{Enc} \quad \text{Dec}
\]

Ideal
AEAD Security Game

\[
\begin{align*}
&\text{Enc, AD, }, \text{ }, \text{ }, \text{ } \\
&\text{Dec, AD, }, \text{ }, \text{ }, \text{ }
\end{align*}
\]
AEAD Security Game

Restriction: Forbidden queries:
- Repetition of nonces
- Ask Dec(A,N,C) after Enc(A,N,M) returned C
Roadmap

- We formulate application-centric security guarantees of AEAD
- We derive a method to judge the security of TLS proposals
- This method can be used to improve existing proposals
Modeling Communication

Interface A — Insecure Channel — Interface B

Interface E
Modeling Communication
What Features should a Secure Channel have?
What Features should a Secure Channel have?

Structure of Packets:

- Header and payload part
  - Header: Version number, type information; Payload: message fragments
What Features should a Secure Channel have?

Structure of Packets:

- Header and payload part
  - Header: Version number, type information; Payload: message fragments

Security requirements:

- Payload is confidential
- Entire packet is authenticated
- Each packet is bound to a certain context
  - E.g.: Version number of the protocol
What Features should a Secure Channel have?

Structure of Packets:

- Header and payload part
  - Header: Version number, type information; Payload: message fragments

Security requirements:

- Payload is confidential
- Entire packet is authenticated
- Each packet is bound to a certain context
  - E.g.: Version number of the protocol

Let us model this as an idealized channel resource!
Augmented Secure Channel

Resource
Augmented Secure Channel

Interface A

Interface E

Interface B
Augmented Secure Channel

Resource
Augmented Secure Channel

Implicit header or context

Interface B

Interface E
Augmented Secure Channel

Implicit header or context

Interface B
Augmented Secure Channel

Implicit header or context

ASC

Interface B

- deliver
- abort

Christian Badertscher | 25.11.2015 | 25
Augmented Secure Channel

Implicit header or context

ASC

Interface B
Augmented Secure Channel

Fetch by providing Implicit header

Implicit header or context
Augmented Secure Channel

Implicit header or context

Successful only with correct context.
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:

\[ \text{A} \rightarrow \text{R} \rightarrow \text{B} \]

The idealized world:

\[ \text{A} \rightarrow \text{S} \rightarrow \text{B} \]
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:

\[ A \xrightarrow{\text{con}_1} R \xrightarrow{\text{con}_2} B \]

\[ E \]

The idealized world:

\[ A \xrightarrow{\text{S}} B \]

\[ E \]
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

  The real world:

  \[ A \xrightarrow{\text{con}_1} R \xrightarrow{\text{con}_2} B \]

  \[ \sim \]

  The idealized world:

  \[ A \xrightarrow{\text{sim}} S \xrightarrow{} B \]
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:

\[ A \xrightarrow{\text{con}_1} R \xrightarrow{\text{con}_2} B \]

The idealized world:

\[ A \xrightarrow{\text{sim}} B \]

Adversarial influence is essentially the same in both worlds
Constructing the Augmented Secure Channel

**Theorem:** Resource ASC can be constructed from a shared key and an insecure channel using a secure AEAD scheme:

- The real world:
  - A → enc → IC → dec → B
  - E → A → enc → IC → dec → B → E

- The idealized world:
  - A → ASC → B
  - E → A → ASC → B → E

\( \approx \)
Details on the Construction

Converter of Alice:

\[ \text{Enc} \text{seq_no} \text{Encode} H \]
Details on the Construction

Converter of Alice:
Details on the Construction

Converter of Bob:

Fetch
Details on the Construction

Converter of Bob:

Diagram showing the process of converting a message with a key and a sequence number.
Details on the Construction

Converter of Bob:
Details on the Construction

**Proof Idea:** Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:
Details on the Construction

**Proof Idea:** Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:
Details on the Construction

**Proof Idea:** Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:
Application of ASC: Sound Design of Practical Protocols
Application of ASC: Sound Design of Practical Protocols

Example: Re-Modelling the TLS 1.3 Record Layer:
Application of ASC: Sound Design of Practical Protocols

Example: Re-Modeling the TLS 1.3 Record Layer:

Our model gives insights into current proposals:
1. The nonce needs no randomness.
2. The sequence number need not be part of the AD.
3. The version number can be part of the implicit header.
Summary

Augmented Secure Channels…

• capture the application semantics of AEAD.
• allow easy security checks of existing protocols.
• allow to develop sound communication protocols in a modular way.
Contact information and credits

ETH Zurich
Department of Computer Science
Universitätsstrasse 6
8092 Zurich

References:


Images: https://openclipart.org/