

# Parsing Ambiguities in Authentication and Key Establishment Protocols

Liqun Chen      HP Labs

Chris Mitchell      Royal Holloway, University of London

29-30 January 2009, Cambridge

1



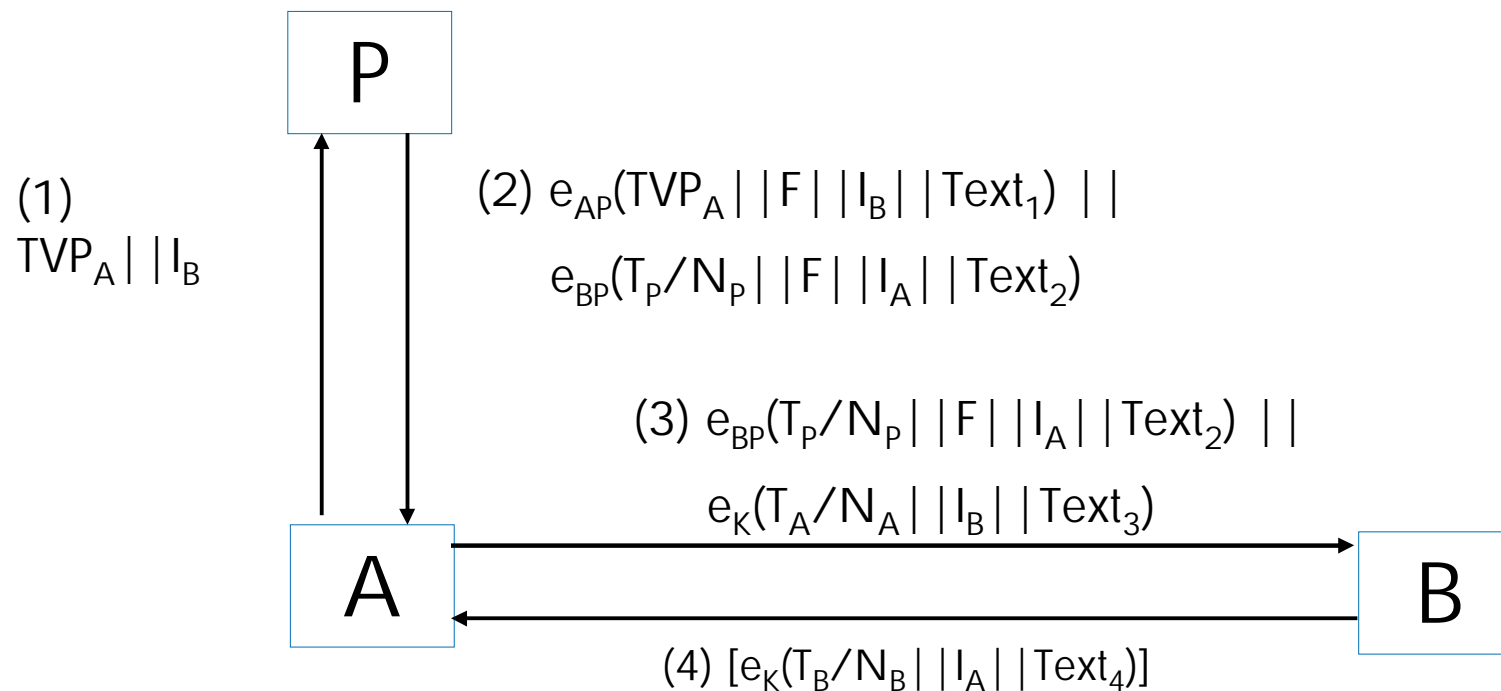
# Outline

- Concept of parsing ambiguities
- Two examples of parsing ambiguity attacks
- Possible generalisations
- Some countermeasures
- Concluding remarks

# What are Parsing Ambiguities?

- $|$  - concatenation -----  
a | | nice | | bar ó an | | ice | | bar
- $m = m_1 | | m_2 = m_3 | | m_4$
- $\text{Enc}_K(m_1 | | m_2) = \text{Enc}_K(m_3 | | m_4)$
- $\text{Sig}_K(m_1 | | m_2) = \text{Sig}_K(m_3 | | m_4)$
- $\text{MAC}_K(m_1 | | m_2) = \text{MAC}_K(m_3 | | m_4)$
- A new class of attacks against authentication and authenticated key establishment protocols
- Affect a large number of International Standards

# Ex1: Mechanism 8 of ISO/IEC 11770-2



At the end of the protocol, A and B share a key K computed from the value F.

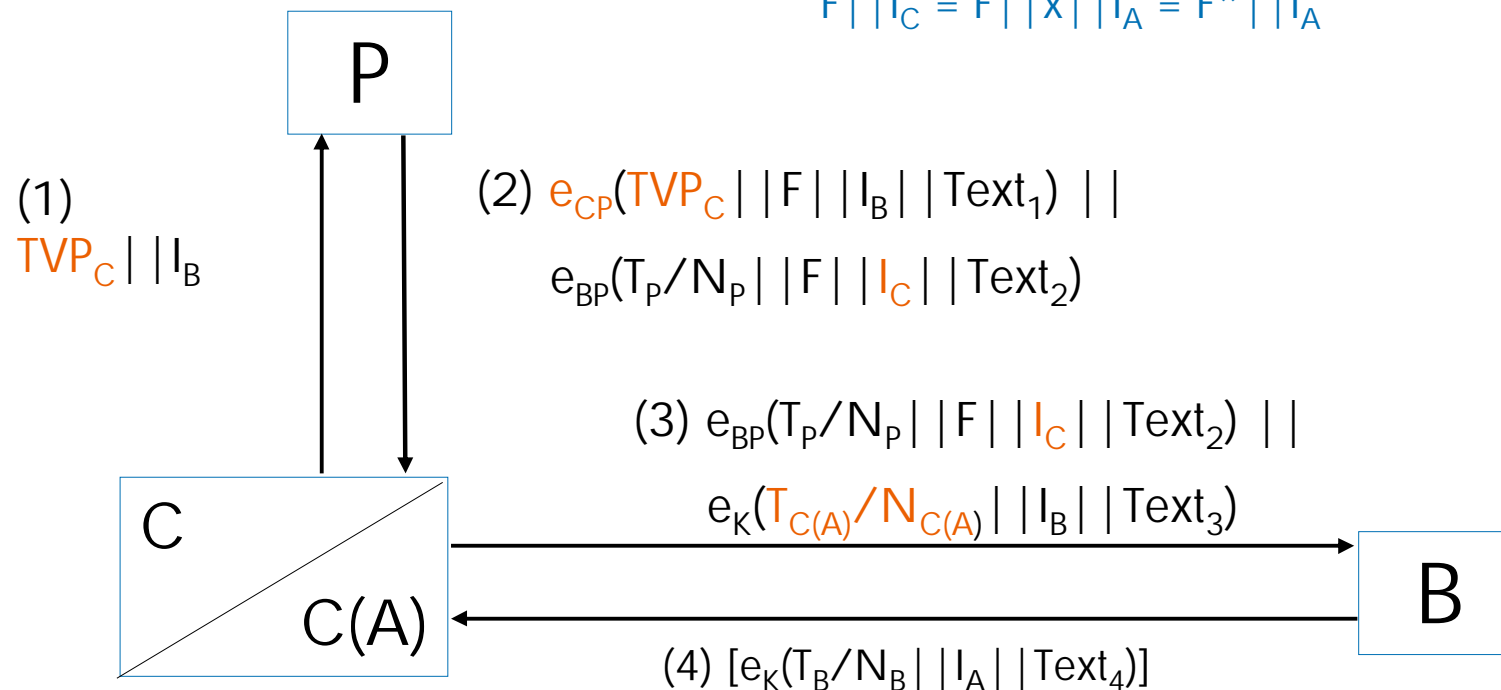


# An attack on the protocol

C chooses  $I_C = x || I_A$ , e.g.

$I_A = \text{a.smith@hp.com}$ ,  $I_C = \text{c.a.smith@hp.com}$

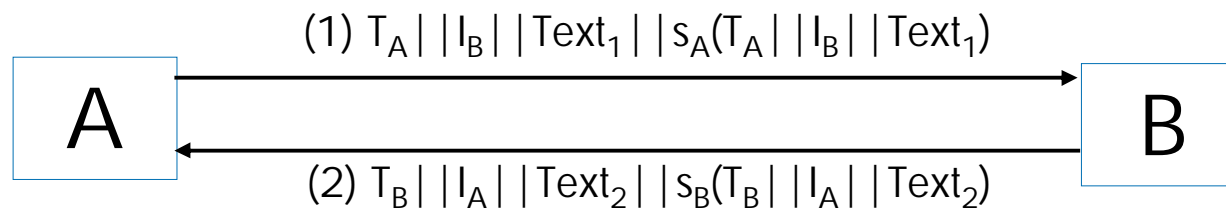
$F || I_C = F || x || I_A = F^* || I_A$



At the end of the protocol, C and B share a key K computed from the value  $F^*$ , but B believes that the key has been shared with A.

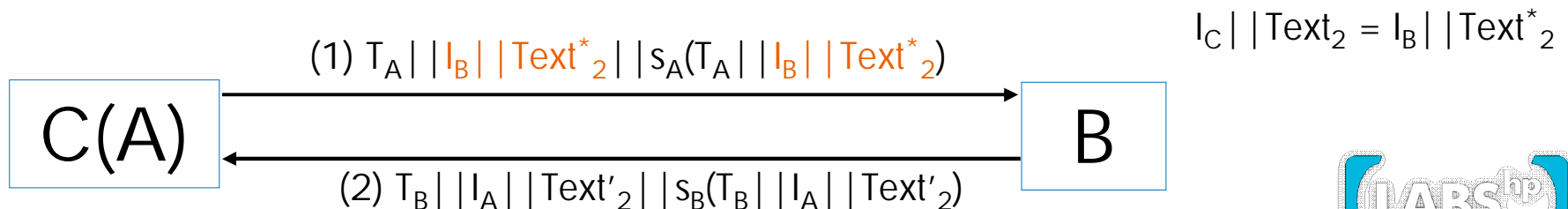
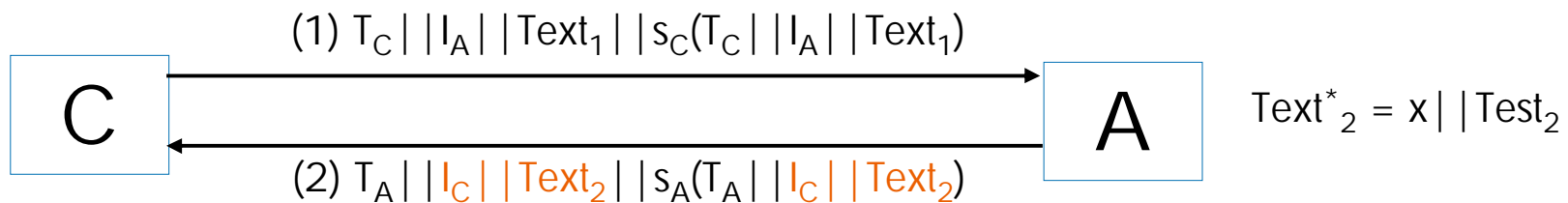


# Ex2: mutual authentication mechanism of ISO/IEC 9798-3



At the end of the protocol, A and B believe that they have been talked to each other.

Attack. C registers  $I_C = I_B || x$ .



# Realising the attacks

The attacks require at least two of the protocol message fields to be of variable length

- Key material fields  $F$  – varying length of keys
- Identifier fields  $I_x$  – arbitrary length
- Optional text fields  $\text{Text}_i$  – application dependent
- Nonces  $R_x$  – varying length – user dependent

# Widening the attack scope

Let's see how widely the attacks apply:

- Any of third-party-based mechanisms in ISO/IEC 11770-2 and ISO/IEC 9798-2
- Majority of two-party protocols in ISO/IEC 9798-2, 9798-3 and 9798-4
- Many public key based mechanisms in ISO/IEC 11770-3, including identity-based mechanisms
- Two authentication protocols in NIST FIPS Pub 196

# Identifying “parsing error”

Possible false interpretation of a cryptographically protected string, not protocol design

- $m = m_1 || m_2 = m_3 || m_4$
- $m_3 || m_4 = \text{Dec}_{K'}(\text{Enc}_K(m_1 || m_2))$
- $\text{Verify}_{K'}(\text{Sig}_K(m_1 || m_2), m_3 || m_4) = \text{OK}$
- $\text{MAC}_K(m_1 || m_2) = \text{MAC}_K(m_3 || m_4)$

# Fixing the problem

- Composing encrypted data strings parsed unambiguously
- Combining data strings as MAC or signature input in a unique way
- Fixing the lengths of each field (Bellare and Rogaway's original assumption in 1995)
- Encoding each substring
- replacing some substring with their digest using collision-resistant hash-functions

# Concluding remarks

- We have just shown one example of issues that can arise when translating theory into practice
- “provable security” doesn’t guarantee the problem free
- Ten ISO/IEC standards are vulnerable to the parsing ambiguity attacks, and seven Technical Corrigendum documents are in their way of development
- The attacks described here by no means the only examples of attacks of this type

Thanks!

