An Updated Threat Model for Security Ceremonies

Marcelo Carlomagno Carlos, Jean Everson Martina,
Geraint Price, Ricardo Felipe Custódio

Royal Holloway University of London
Information Security Group, United Kingdom

Universidade Federal de Santa Catarina
Departamento de Informática e de Estatística, Brazil

{marcelo.carlos.2009, geraint.price}@rhul.ac.uk,
{everson, custodio}@inf.ufsc.br

Contents

Introduction

Historical facts

- Needham and Schroeder introduced the idea of an active attacker in 1978 [NS78] who could:
  - Modify messages
  - Copy messages
  - Replay messages
  - Create messages
- Dolev and Yao further developed the attacker model [DY83]
  - **The attacker has complete control of the communication channels (respecting cryptography)**
- Nowadays, the Dolev-Yao threat model is the most widely accepted model to analyse security protocols

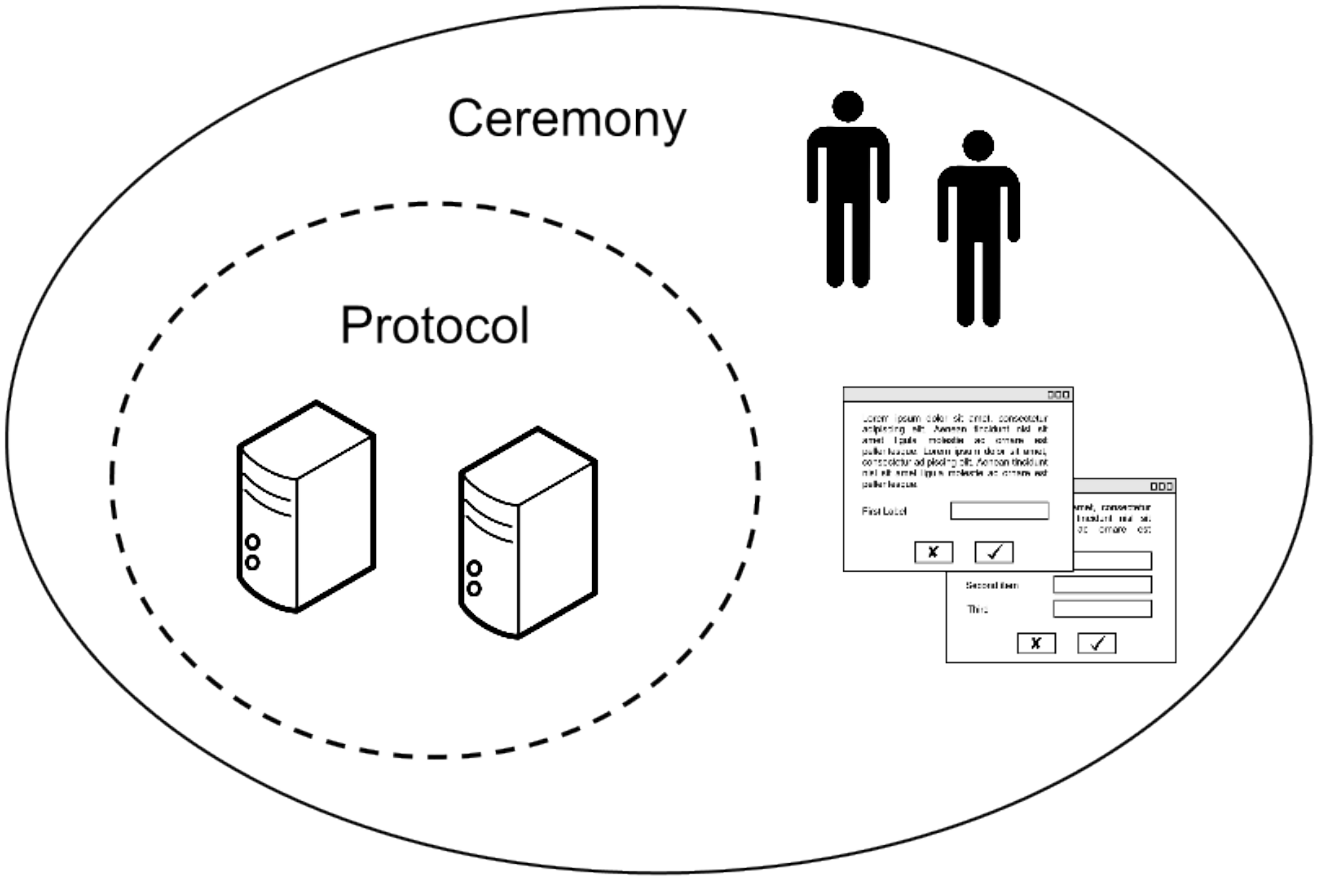
Introduction

Motivation

- When put in practice, protocols' assumptions that involves human-device and human-human interaction have to be implemented
- They are then replaced by dynamic user-interactions
- Even protocols verified under Dolev-Yao threat model assumptions might be susceptible to attacks when implemented due to some reasons, which may include:
  - Clear usability problems – the user must have unrealistic capabilities to perform his activities
  - The assumptions are too big/strong or too generic – it is often necessary to assume that previous steps were successfully performed, or that the user is capable of performing some kind of operation

Security Ceremonies

Ellison introduced the concept of a broader view to security protocols called “ceremony” [Ell07]



Security Ceremonies

- A ceremony allows more detailed analysis of a protocol
- Assumptions are more precise and well described
- A Dolev-Yao attacker for ceremonies is not always consistent with real world threats
  - An attacker capable of modifying (or replaying) a "speech" packet in a human-human medium is unrealistic if this communication happens in person
- The description attacker capabilities for ceremonies scope requires finer granularity in its description

Security Ceremonies

- If a ceremony is secure against a Dolev-Yao attacker, the same ceremony will be secure against a weaker attacker
- However, to guarantee that a ceremony is secure against a such powerful attacker, we have to include very complex mechanisms
- By doing that, a new threat is introduced, which is the fact that the user is likely to try to circumvent the security mechanisms in order to accomplish his/her tasks
- A more realistic threat model can prevent the user from being overloaded, and consequently make the ceremony more usable and secure

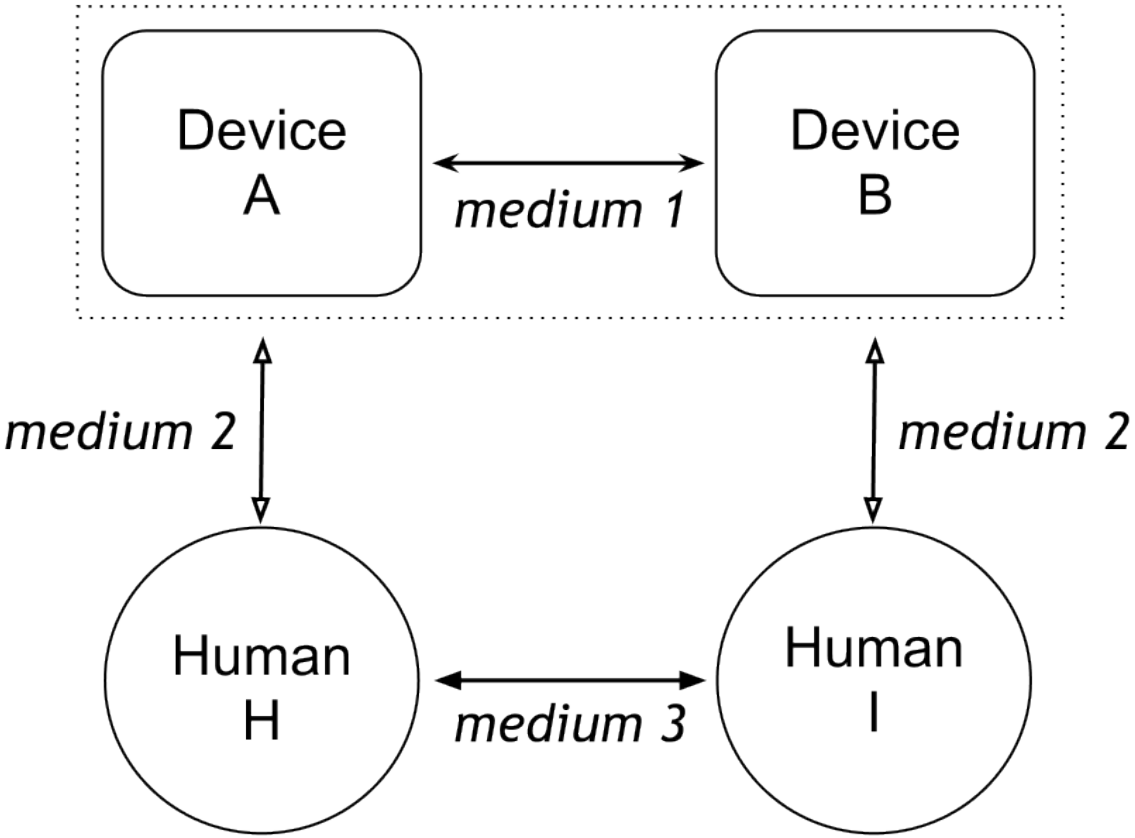
Premises for Ceremonies Threat Modelling

- No being is omnipotent in human-human channels
- Omnipotency in the human-device channel is not always realistic
- A threat model including human peers should be constrained by the laws of physics
- Humans are capable of performing basic information recall or mathematical operations
- One should never use more crypto than needed

Proposed Threat Model

Scenario

- We introduce two new possible communication channels.



Proposed Threat Model

- Considering worst case is not always the best option since it degrades usability
- The threat model must be adaptive
- For network communication (device-device channel) we will usually assume a Dolev-Yao attacker
- A threat model for ceremonies must be ceremony-dependent and context-dependent

Proposed Threat Model

Proposition

- We start from Dolev-Yao, and then we remove one or more capabilities from the attacker
- Our final goal is to measure the security of ceremonies against a Dolev-Yao attacker with a smaller set of capabilities
- This approach will also help us to reuse some of the abstract verification techniques and tools already in use for security protocols
- Verify that ceremonies are secure against a realistic attacker

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate
- Atomic Break Down
- Crypto
- Block
- Fabricate
- Spoof
- re-Order

Some of the characteristics are not directly shown here, since they can be achieved by the combination of our definitions (e.g. Replaying = Eavesdrop + Initiate)

Example scenario: Bluetooth Pairing Protocol

Overview

- Protocol designed to allow one device to recognise and connect to another.
- Our focus is on the **Secure Simple Pairing (SSP)** (bluetooth 2.1 onwards) using the **Numeric Comparison** mode:
  - designed for devices capable of displaying digits (a six digit number) and accepting user inputs ("yes" or "no")
  - The device displays six digit numbers on both devices and the users are asked whether the numbers are the equal on both devices.
  - If the digits are equal, the pairing is successful

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Numeric Comparison

Ceremony

Protocol

M1.	B	$\xrightarrow[DD]{}$	A	:	$C_b = f1(pk_B, pk_A, N_b, 0)$
M2.	A	$\xrightarrow[DD]{}$	B	:	N_a
M3.	B	$\xrightarrow[DD]{}$	A	:	N_b

Assumptions

M4.	A	$\xrightarrow[HD]{}$	U_A	:	$V_a = g(pk_A, pk_B, N_a, N_b)$
M5.	B	$\xrightarrow[HD]{}$	U_B	:	$V_b = g(pk_A, pk_B, N_a, N_b)$
M6.	U_A	$\xrightarrow[HH]{}$	U_B	:	V_a
M7.	U_B	$\xrightarrow[HH]{}$	U_A	:	V_b

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

Theorem (Numeric Comparison + DY)

If the protocol messages M_1 to M_7 are run against a DY attacker, the attacker can prevent U_A from learning V_a or V_b and U_B from learning V_b or V_a, forcing them to learn V_i instead.

$$\frac{M_{1\ldots7} \cup DY}{\begin{array}{r} V_a \wedge V_b \wedge V_i \in knows(I) \wedge \\ V_a \notin knows(A) \wedge V_b \notin knows(A) \wedge \\ V_b \notin knows(B) \wedge V_a \notin knows(B) \wedge \\ V_i \in knows(U_A) \wedge V_i \in knows(U_B) \end{array}}$$

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis – NC + DY

- Assuming the attacker I initiated two parallel pairing sessions with A and B during Messages M_1 to M_3:

$$
\begin{array}{llcll}
\text{M4.} & A & \xrightarrow[HD]{} & U_A & : \quad V'_a = g(pk_A, pk_I, N_a, N_i) \text{ (Blocked)} \\
\text{M5.} & B & \xrightarrow[HD]{} & U_B & : \quad V'_b = g(pk_I, pk_B, N_i, N_b) \text{ (Blocked)} \\
\text{M4'.} & I & \xrightarrow[HD]{} & U_A & : \quad V_i \text{ (Chosen by the attacker)} \\
\text{M5'.} & I & \xrightarrow[HD]{} & U_B & : \quad V_i \text{ (Chosen by the attacker)} \\
\text{M6.} & U_A & \xrightarrow[HH]{} & U_B & : \quad V_i \\
\text{M7.} & U_B & \xrightarrow[HH]{} & U_A & : \quad V_i
\end{array}
$$

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

- Although first attack described is plausible in real world scenarios, it is very difficult to be deployed
- An attacker would have to corrupt both devices as well as start parallel sessions with both users during a short period of time
- By removing capabilities “Block” and “Initiate” from the attacker, we can analyse the protocol further, and possibly find other (more) relevant attacks

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

Theorem (Numeric Comparison + Ad. Threat Model V1)

If the protocol messages M_1 to M_3 are run against a DY attacker; the messages M_4 to M_5 are run against a N+E attacker; and messages M_6 to M_7 are run against a DY attacker, the attacker can prevent U_A from learning V_b and U_B from learning V_a, forcing them to learn the repetition (replay) of V_a and V_b (respectively) instead.

$$\frac{(M_{1\ldots3} \cup DY) \wedge (M_{4\ldots5} \cup N + E) \wedge) (M_{6\ldots7} \cup DY)}{V_a \wedge V_b \in knows(I) \wedge V_a \notin knows(B) \wedge V_b \notin knows(A)}$$

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

- Assuming the attacker I initiated two parallel pairing sessions with A and B during Messages M_1 to M_3:

M4.	A	$\xrightarrow[HD]{}$	U_A	:	$V'_a = g(pk_A, pk_I, N_a, N_i)$
M5.	B	$\xrightarrow[HD]{}$	U_B	:	$V'_b = g(pk_I, pk_B, N_i, N_b)$
M6.	U_A	$\xrightarrow[HH]{}$	U_B	:	V'_a (Blocked)
M7.	U_B	$\xrightarrow[HH]{}$	U_A	:	V'_b (Blocked)
M6'.	I	$\xrightarrow[HH]{}$	U_B	:	V'_b ($V'_b \in knows(I)$ by M5 or M7)
M7'.	I	$\xrightarrow[HH]{}$	U_A	:	V'_a ($V'_b \in knows(I)$ by M4 or M6)

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

- This second attack is completely unrealistic
- The attacker would have to block a communication between two humans and then replay some data over a channel where the user would easily notice if some other party wanted to spoof the identity of the sender
- In this case, the attack does not exist in practice

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

Theorem (NumComp + Ad. Threat Model V2)

If the protocol messages M_1 to M_3 are run against a DY attacker and the messages M_4 to M_7 are run against a N+E attacker the attacker cannot produce any relevant attack.

$$\frac{(M_{1...3} \cup DY) \wedge (M_{4...7} \cup N + E)}{\emptyset}$$

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

- Assuming the attacker I initiated two parallel pairing sessions with A and B during Messages M_1 to M_3:

$$
\begin{array}{lccccc}
\text{M4.} & A & \xrightarrow[HD]{} & U_A & : & V'_a = g(pk_A, pk_I, N_a, N_i) \\
\text{M5.} & B & \xrightarrow[HD]{} & U_B & : & V'_b = g(pk_I, pk_B, N_i, N_b) \\
\text{M6.} & U_A & \xrightarrow[HH]{} & U_B & : & V'_a \\
\text{M7.} & U_B & \xrightarrow[HH]{} & U_A & : & V'_b
\end{array}
$$

The attack fails

Since $V'_a \neq V'_b$ and the attacker cannot initiate communication using the *HD* and *HH* channels, there is no realistic attack on the protocol.

Gains Under a Realistic Threat Model

- The misunderstanding of the correct threat model would lead to us to the incorrect conclusion of the protocol (and related ceremony) is not secure
- The ceremony for the bluetooth association protocol can be described avoiding these conclusions
- The ceremony could enforce the use of a correct threat model choice at implementation level
- Example: an application could dynamically allow/block different association modes depending on the environment
- This kind of ceremony potentially trains users to detect different threat models

Concluding Remarks

- The use of a worst-case scenario threat model is justifiable in security protocol scenarios
- However, the same cannot be said for security ceremonies
- Human agents executing security ceremonies are constrained by the laws of physics and usual capabilities expected from human beings
- The existence of a extremely powerful agent is not plausible in some real-world scenarios

Concluding Remarks

- Our approach is based on a well established model for security protocols
- We weaken the attacker to match the premises for human-device interaction and human-human interaction
- Our model helps security protocols and ceremony designers to develop ceremonies:
  - using reasonable assumptions
  - tailored to the real capabilities of the attacker
  - that do not contain unnecessary protection mechanisms to unrealistic attacks

Concluding Remarks

Future Work

- Specification of the threat model using an abstract verification method
- Automation for testing and design of security ceremonies

Thank you!

Questions?

References


Danny Dolev and Andrew C. Yao, *On the security of public key protocols*, IEEE Trans. on Inform. Theory **29** (1983), no. 2, 198–208.


Carl Ellison, *Ceremony Design and Analysis*, Cryptology ePrint Archive, Report 2007/399, October 2007.


Roger M. Needham and Michael D. Schroeder, *Using encryption for authentication in large networks of computers*, Comm. of ACM **21** (1978), no. 12, 993–999.