Carlos-Martina et al. Security Ceremonies

Design and Verification of Security Protocols and Security Ceremonies

Programa de Pós-Graduacão em Ciências da Computacão
Dr. Jean Everson Martina

August-November 2016

Programa de Pós-Graduação em Ciência da Computação UFSC

UNIVERSIDADE FEDERAL DE SANTA CATARINA

Introduction

Historical facts

- Needham and Schroeder introduced the idea of an active attacker in 1978;
  - Alter;
  - Copy;
  - Replay;
  - Create messages (or parts of messages) in all communication paths
- Dolev and Yao (1983) further developed this attacker model by formalising it and adding new assumptions.
  - Has complete control of the network but is not able to perform cryptanalysis.

Introduction

Current Facts

- Even protocols verified under Dolev-Yao threat model assumptions might be susceptible to attacks when implemented.
- Why?
- Used by humans?
  - Non-deterministic nature of human behaviour.
  - Problems happen not due to a design flaw or user's misconduct.
  - But due to the implementation of a protocol assumption.
- How to include humans in the design and verification of security Protocols?

- Ellison introduced the concept of a broader view to security protocols, and called it a “ceremony”.
- A ceremony is an extension to the network protocol, its nodes may be humans or computers, and the communication channels are not limited to the network.
- Doing so we can understand better the assumptions for protocols.
- We may even be able to do some formal verification of such things in the future.

Introduction

Argument

- Dolev-Yao's threat model can represent the most powerful attacker possible.
- But, the attacker in this model is not realistic in certain scenarios.
- Protocols fail when implemented is because their assumptions are either not well specified or not realistic.
- Workarounds may introduce security problems.
- Despite the fact that the problem was created during the implementation, its cause was an inaccurate assumption forced by an unrealistic threat model.

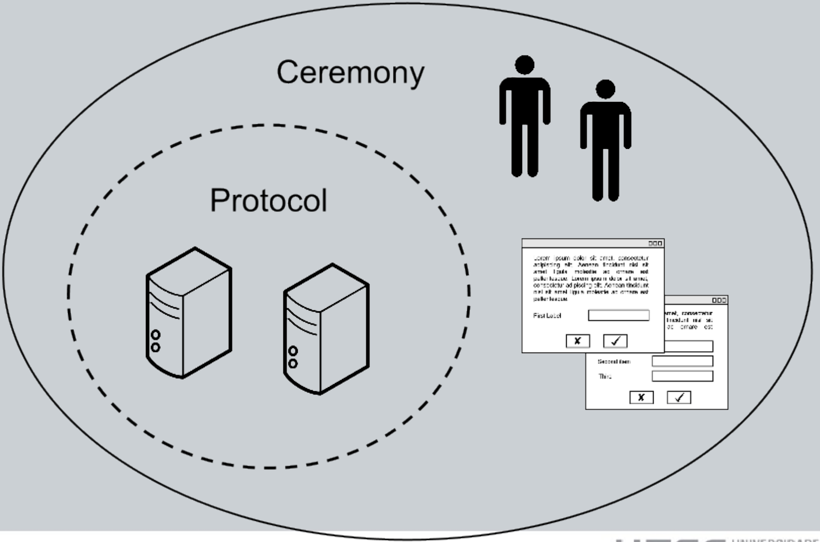
Ceremony versus Protocol

- Security protocols are sequence of interactions among entities designed to achieve a certain end.
- Goals are (not limited to):
  - Authentication,
  - Key distribution,
  - Secrecy,
  - Anonymity, etc.

Ceremony versus Protocol

- Include additional node types,
- Communication channels,
- And operations which were previously out-of-bounds
- Examples:
  - User interaction
  - Pre-key distribution

Ceremony versus Protocol



Ceremony versus Protocol

- By including a human node, we have to define and use extra mediums such as:
  - User-interfaces for human-device interaction,
  - A human medium, to represent speech, gestures, etc, for human-human interaction.
- In a protocol specification, we define assumptions to represent out-of-bound operations.
- In ceremonies we break down these assumptions into smaller and well described assumptions

Ceremony Verification

- A ceremony allows a more detailed analysis of a protocol.
- The capabilities of an attacker under a ceremony scope requires finer granularity in its description.
- Dolev-Yao for ceremonies they are not always consistent with real world threats.
- For example:
  - An attacker capable of modifying (or replaying) a “speech” packet in a human-human medium is unrealistic if this communication happens in person.

Ceremony Verification

Justification

- A more human-centric security view.
- Designing more realistic ceremonies.
- Assist the human peer to assess the threat level he is subject to.
- By not overstating assumptions we inherently make them plausible and achievable.

Premises for Ceremonies

Weaker Dolve-Yao

- If secure against a Dolev-Yao attacker the same ceremony will be secure against any weaker real-world attacker.
- But to guarantee that a certain 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 will 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

Premise One

- No being is omnipotent in human-human channels.
  - Detection of powers beyond usual human capability is straightforward in the setting of security ceremonies
  - Depending on the situation, the presence of an active attacker is not realistic.
  - Ex.: replaying or blocking “speech” in a human-to-human channel will involve the use of powers that are not feasible for a human peer.

Premises for Ceremonies

Premise Two

- Omnipotency in the human-device channel is not always realistic
  - We expect that an attacker has full control over the human-device channel.
  - In some specific situations such a powerful attacker does not represent reality.
  - The capabilities of the attacker over the human-device are limited.
  - Ex.: a ceremony that makes use of single-purpose devices (e.g. one-time password generators).

Premises for Ceremonies

Premise Three

- A threat model including human peers should be constrained by the laws of physics.
    - It is unrealistic to assume an omnipresent attacker in human-human channels.
    - Human peers can properly choose a location to execute their ceremonies taking into account the verifiable presence of a potential attacker.
    - Ex.: A real world example of such premise is execution of security ceremonies for PKIs in safe rooms with strict physical and electromagnetic controls.

Premises for Ceremonies

Premise Four

- Humans are capable of performing basic information recall or mathematical operations.
  - Human peers are required to recall just fresh information and to execute basic mathematical operations.
  - It impacts on how the personification of the attacker in the human-human channel behaves.
  - Ex.: An example is the possession of a device in an authentication scenario to generate one-time passwords.

Premises for Ceremonies

Premise Five

- One should never use more crypto than needed.
  - Noted by Anderson and Needham a long time ago.
  - May induce the human who is taking part in the ceremony to misunderstand the threat level he is subject to
  - Ex.: An example of such extra layer not addressing the threat model is the usage of One-Time Password authentication devices by banks.

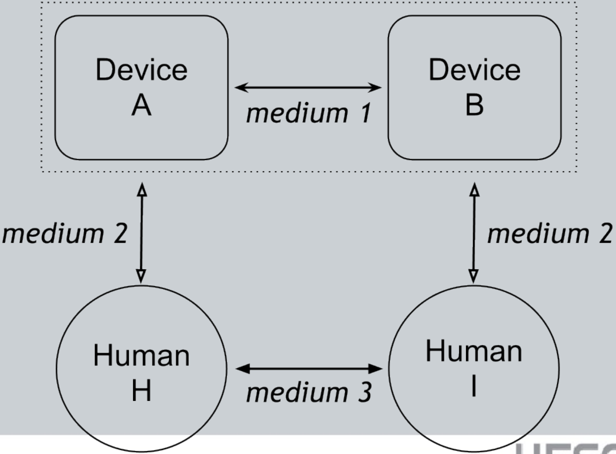
Proposed Threat Model

Justification

- Reasons for insecurity are not directly related to the network channel.
- Therefore the protocol is secure.
- We cannot make the same statements when the protocol is implemented.
- We cannot assure that the expected security properties assumed in the protocol design will hold in the ceremony.

Proposed Threat Model

- We introduce two new possible communication channels.



Proposed Threat Model

We also consider...

- Humans make different decisions regarding their security based on a dynamic evaluation of the threat level they are subject in the environment.
    - The pressure humans suffered to decide whether to engage into attacks to become hunters or keep a way of life of gatherers.
    - Inherent faculty of human nature is usually not taken into account when we always assume the worst case scenario.
    - Some attacks may be thwarted by using an over pessimistic threat model, but inherently this action will attract the human nature to act and find an easier and plausible solution.

Proposed Threat Model

Proposition

- The threat model must be adaptive.
- Considering worst case is not always the best option since it degrades usability.
- For network communication (device-device channel) we will always assume a Dolev-Yao.
- A threat model for ceremonies must be ceremony and context-dependent.
- The existence of a standardised threat model scenario is paramount to the establishment of security goals of ceremonies.

Proposed Threat Model

Porposal

- We start from Dolev-Yao, and then we remove one or more capabilities of 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 ceremonies that are secure against a realistic attacker with different capabilities under different channels.

Proposed Threat Model

Notation

- "DY" is a Dolev-Yao attacker
- "DY-BR" means a Dolev-Yao attacker without the blocking and replaying capabilities.
- All the logical connectives have their usual meaning.
- The set knows(X), represents the set of knowledge of an agent X in the protocol.

Proposed Threat Model

Capabilities

Definition (Eavesdrop – E)

$$\forall X \in M.\ A \rightarrow B : X \Rightarrow X \in knows(I)$$

Definition (Initiate – I)

$$\forall X \in \mathit{knows}(I).\ I \rightarrow B : X$$

Definition (Atomic Break Down – A)

$$\forall \{X, Y\} \in knows(I). \Rightarrow$$
$$\{X\} \in knows(I) \ \wedge \ \{Y\} \in knows(I)$$

Proposed Threat Model

Capabilities

Definition (Crypto – C)

$$\forall \{X\}_k \in M \wedge\ k \in knows(I).\ A \rightarrow B : \{X\}k \Rightarrow X \in knows(I)$$

Definition (Block – **B**)

$$\forall X \in M.\ A \rightarrow B : X \Rightarrow X \notin knows(B)$$

Proposed Threat Model

Definition (Fabricate – **F**)

$$\forall X \in knows(I) \Rightarrow F(X) \in knows(I)$$

- Examples of such functions can be cryptographic hashes, public-key encryption, or any other function publicly available to the execution of the ceremony.

Definition (Spoof – **S**)

$$\forall X \in \mathit{knows}(I).\ \mathit{Spoof}(I, A) \rightarrow B : X$$

- Spoof differentiates from Initiate in deliberately not allowing the attacker to be an internal agent in the execution of the ceremony.

Proposed Threat Model

Capabilities

Definition (re-Order – **O**)

$$\forall X, Y \in M.\ A \rightarrow B : X \ \wedge \ C \rightarrow B : Y \Rightarrow$$
$$Y \in knows(B) \ \wedge \ ... \ \wedge \ X \in knows(B)$$

- An important notice to this capability is that it is described from the receiver's point of view, since there are many different ways of the Intruder achieving it.

Proposed Threat Model

Capabilities

- Some of the characteristics are not directly shown here, since they can be achieved by the combination of our definitions
- Examples:
  - Modifying (M) messages on the communication channels can be defined as the use of **Block** + **Initiate**
  - Replaying (R) messages can be represented as **Eavesdrop** + **Initiate** or **Eavesdrop** + **Spoof**

Proposed Threat Model

Secondary Notation

- We start with no threat model.
- The attacker has "no capabilities" (N).
- We add to the (N) attacker the desired capabilities.
- Examples:
  - N + E for eavesdrop only,
  - N + EB for eavesdrop and block only.
- DY-IDBRSM = N+E

Example scenario: Bluetooth Pairing Protocol

- Protocol designed to allow one device to recognise and connect to another.
- There are two variations of the pairing protocol
  - Legacy Pairing – bluetooth version 1.0 to 2.0 [**?**]
  - Secure Simple Pairing (SSP) – bluetooth 2.1 onwards [**?**]

Example scenario: Bluetooth Pairing Protocol

Legacy Pairing

- Pairing is performed in a way where both devices are required to enter a common PIN to establish the connection
- Three input types:
  - Fixed PIN number is used (e.g. 1234)
  - Numeric input
  - Alpha-numeric input

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP)

- Solves several flaws that allowed attackers to deploy man-in-the-middle (MITM) attacks on earlier versions
- Defines four different association modes
- Simplifies the pairing process from the user's point of view

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP)

- SSP association modes:
  - **Numeric Comparison**
  - Just Works
  - Out of band (OOB)
  - Passkey entry

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP)

- 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

- The association modes are designed under assumptions that imply in a weaker threat model for the pairing protocol.
- Legacy mode
  - Device-device medium (DD) is designed considering a DY attacker
  - Human-device (HD) and human-human mediums (HH) are assumed to have no attackers.
  - A ceremony analysis can easily find an attack if we add the capability of eavesdropping to the attacker on either HD or HH mediums.
  - The attacker learns the PIN by eavesdropping those mediums (hearing the PIN value) and with that, he can

Example scenario: Bluetooth Pairing Protocol

- The association modes are designed under assumptions that imply in a weaker threat model for the pairing protocol.
- SSP
  - Each association mode also needs to be analysed under a different threat model
  - We will focus on the numeric comparison mode

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Numeric Comparison

$$
\begin{array}{llcll}
\text{M1.} & B & \xrightarrow[DD]{} & A & : & C_b = f1(pk_B, pk_A, N_b, 0) \\
\text{M2.} & A & \xrightarrow[DD]{} & B & : & N_a \\
\text{M3.} & B & \xrightarrow[DD]{} & A & : & N_b \\
\text{M4.} & A & \xrightarrow[HD]{} & U_A & : & V_a = g(pk_A, pk_B, N_a, N_b) \\
\text{M5.} & B & \xrightarrow[HD]{} & U_B & : & V_b = g(pk_A, pk_B, N_a, N_b) \\
\text{M6.} & U_A & \xrightarrow[HH]{} & U_B & : & V_a \\
\text{M7.} & U_B & \xrightarrow[HH]{} & U_A & : & V_b
\end{array}
$$

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_b and U_B from learning V_a, forcing them to learn V_i instead.

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

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

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

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

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:

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

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.

$$\frac{(M_{1\ldots3} \cup DY) \wedge (M_{4\ldots7} \cup N + E)}{\emptyset}$$

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:

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

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.

Example scenario: Bluetooth Pairing Protocol

Secure Simple Pairing (SSP) – Analysis

- Although the 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 B and I of 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

- The 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.

Gains Under a Realistic Threat Model

- The misunderstanding of the correct threat model would lead to us to two types of incorrect conclusions in the SSP Protocol:
  - The protocol (and related ceremony) is not secure due to the fact they do not cope with an over-pessimistic threat model.
  - The protocol is secure, but the user misunderstands the evaluation of the correct threat he is subject to.

Gains Under a Realistic Threat Model

- The ceremony for the bluetooth association protocol can be described avoiding these conclusions.
- The ceremony could enforce the correct threat model choice at implementation level.
- The application would dynamically allow/block association modes depending on the environment

Gains Under a Realistic Threat Model

- Pairing under the JW mode:
  - The application should scan the area and check whether there are more bluetooth enabled devices around.
  - If more than one is found, the JW mode should not be available.
  - If only one device is found, the JW mode can be securely used.

Gains Under a Realistic Threat Model

Other Working Examples

- Other ceremonies we are working:
  - ATM authentication ceremonies
  - TLS handshake protocol implementations

Final Remarks

Conclusions

- The existence of a single 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.
- The existence of a such powerful agent is not plausible.

Final Remarks

Conclusions

- Our approach is based on a well established model for security protocols
- We weaken the attacker to conform to the premises governing human-device interaction and human to human interaction.
- Helps security protocols and ceremony designers to develop ceremonies with reasonable assumptions
- Tailored to the real capacities of the attacker.

Final Remarks

Future Work

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

References

Discussion

-

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA