Advanced Threat Models for Symbolic Evaluation

Design and Verification of Security Protocols and Security Ceremonies

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

March-June 2018

Programa de Pós-Graduação em Ciência da Computação UFSC

UNIVERSIDADE FEDERAL DE SANTA CATARINA

Disclaimer

Disclaimer!

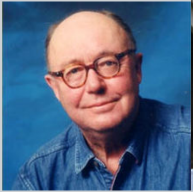
This is not a Lecture, but a keynote I given in CSF 2013 in New Orleans for a workshop called STAST 2013.

Introduction

Historical facts

- Needham and Schroeder introduced the idea of an active attacker in 1978 who could:

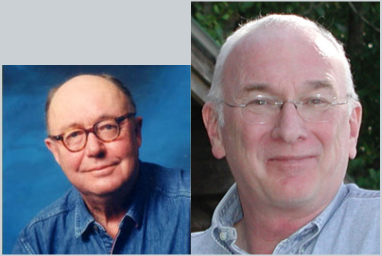
- Needham and Schroeder introduced the idea of an active attacker in 1978 who could:



Introduction

Historical facts

- Needham and Schroeder introduced the idea of an active attacker in 1978 who could:
    - Modify messages;
    - Copy messages;
    - Replay messages;
    - Create messages.



Introduction

Historical facts

- Dolev and Yao further developed the attacker model;

- Dolev and Yao further developed the attacker model;
  - ***The attacker has complete control of the communication channels (respecting cryptography)***;

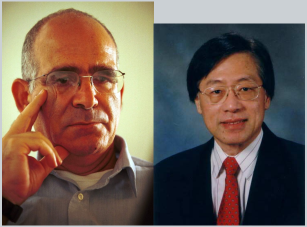
Introduction

Historical facts

- Dolev and Yao further developed the attacker model;
    - ***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

Historical facts



- Dolev and Yao further developed the attacker model;
    - ***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;

Human-centered computing

Definitions

- Concerned with computing as it relate to human condition;

Human-centered computing

Definitions

- Concerned with computing as it relate to human condition;
- Research in human-centred computing has multiple goals;

Human-centered computing

Definitions

- Concerned with computing as it relate to human condition;
- Research in human-centred computing has multiple goals;
- Focus on the ways that human beings adopt, adapt, and organise their lives around computational technologies;

Human-centered computing

Definitions

- Concerned with computing as it relate to human condition;
- Research in human-centred computing has multiple goals;
- Focus on the ways that human beings adopt, adapt, and organise their lives around computational technologies;
- This inherently brings a social aspect to computing!

Introduction

Motivation for Human Centric Protocol Security

- When put in practice, protocols' assumptions that involves human-device and human-human interaction have to be implemented;

Introduction

Motivation for Human Centric Protocol Security

- 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:

- 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;

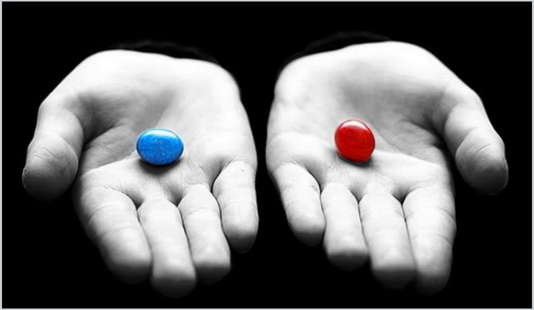
Introduction

Motivation for Human Centric Protocol Security

- 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.

Introduction

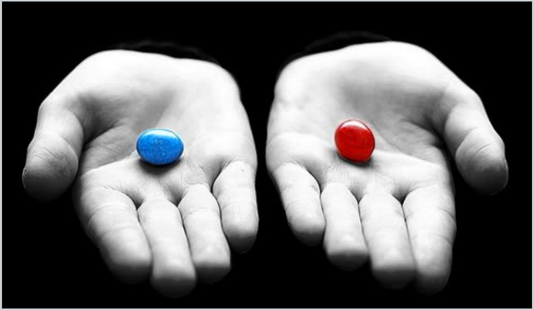
How do we sort this out?



- Clearly we have at least two choices:

Introduction

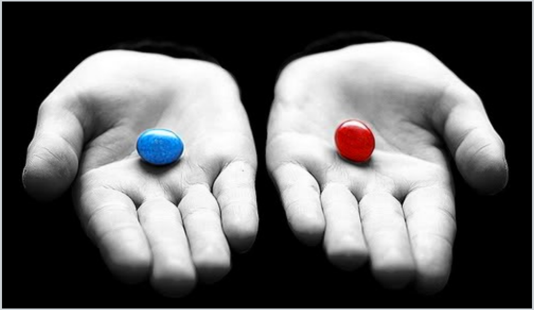
How do we sort this out?



- Clearly we have at least two choices:
  - We change the user interaction;

Introduction

How do we sort this out?



- Clearly we have at least two choices:
  - We change the user interaction;
  - We change the assumption.

Introduction

Why changing the user is not a good idea?

- User interaction is per se unpredictable;

Introduction

Why changing the user is not a good idea?

- User interaction is per se unpredictable;
- Modelling the user is very hard;

Introduction

Why changing the user is not a good idea?

- User interaction is per se unpredictable;
- Modelling the user is very hard;
- Constructing a tool for that is complicated;

Introduction

Why changing the user is not a good idea?

- User interaction is per se unpredictable;
- Modelling the user is very hard;
- Constructing a tool for that is complicated;
- The user is not part of the problem, but part of the solution!

- Dolev-Yao threat model represents the most powerful attacker possible;

- Dolev-Yao threat model represents the most powerful attacker possible;
- However, this powerful attacker is not realistic in certain scenarios;

- Dolev-Yao threat model represents the most powerful attacker possible;
- However, this powerful attacker is not realistic in certain scenarios;
- Workarounds to protect agains unrealistic attacks may introduce security problems;

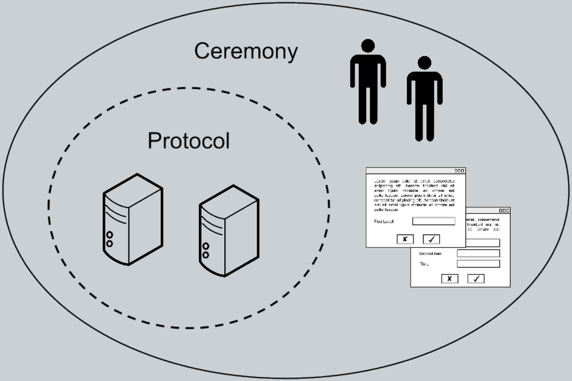
- Dolev-Yao threat model represents the most powerful attacker possible;
- However, this powerful attacker is not realistic in certain scenarios;
- Workarounds to protect agains unrealistic attacks may introduce security problems;
- Despite the fact that the security flaws are introduced during the implementation of the procotol, its cause is often an inaccurate assumption which may have been forced by an unrealistic threat model

Security Ceremonies

Ellison introduced the concept of a broader view to security protocols called "ceremony"

Security Ceremonies

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



Ceremonies

- Security protocols are sequence of interactions among entities designed to achieve a certain end;

Ceremonies

- Security protocols are sequence of interactions among entities designed to achieve a certain end;
  - Goals are (not limited to):

Ceremonies

- 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

Ceremonies

- 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
- Ceremonies include in addition to protocols:

Ceremonies

- 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
- Ceremonies include in addition to protocols:
  - new node types (humans, user interfaces, etc);

Ceremonies

- 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
- Ceremonies include in addition to protocols:
  - new node types (humans, user interfaces, etc);
  - new communication channels (human-device, human-human);

Ceremonies

- 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
- Ceremonies include in addition to protocols:
  - new node types (humans, user interfaces, etc);
  - new communication channels (human-device, human-human);
  - additional operations which were previously out-of-bounds (user interaction, pre-key distribution).

Ceremonies

- 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
- Ceremonies include in addition to protocols:
  - new node types (humans, user interfaces, etc);
  - new communication channels (human-device, human-human);
  - additional operations which were previously out-of-bounds (user interaction, pre-key distribution).
- In a protocol specification, we define assumptions to represent out-of-bound operations;

Ceremonies

- 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
- Ceremonies include in addition to protocols:
  - new node types (humans, user interfaces, etc);
  - new communication channels (human-device, human-human);
  - additional operations which were previously out-of-bounds (user interaction, pre-key distribution).
- 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.

Security Ceremonies

- A ceremony allows more detailed analysis of a protocol

Security Ceremonies

- A ceremony allows more detailed analysis of a protocol
- Assumptions are more precise and well described

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

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

Ceremony Verification

Justification

- A more human-centric security view;

Ceremony Verification

Justification

- A more human-centric security view;
- Designing more realistic ceremonies;

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;

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.

Security Ceremonies

- If a ceremony is secure against a Dolev-Yao attacker, the same ceremony will be secure against a weaker attacker;

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.

Security Ceremonies

- 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;

Security Ceremonies

- 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;

Premises for Ceremonies Threat Modelling

- No being is omnipotent in human-human channels;
- Omnipotency in the human-device channel is not always realistic;

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;

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;

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.

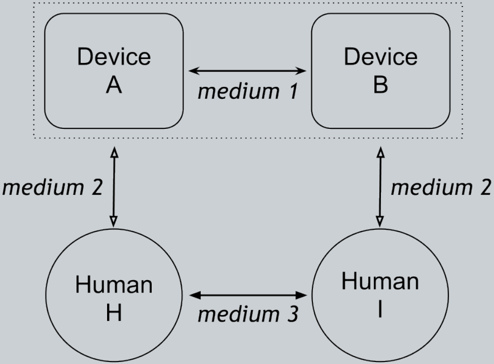
The Ever Changing Threat Model

- We introduce two new possible communication channels.

The Ever Changing Threat Model

Scenario

- We introduce two new possible communication channels.



Proposed Threat Model

We also consider...

- Humans make decisions regarding their security based on the evaluation of the threat level they are subject to:

Proposed Threat Model

We also consider...

- Humans make decisions regarding their security based on the evaluation of the threat level they are subject to:
  - Humans had to decide whether to engage into attacks to become hunters or keep a way of life of gatherers;

Proposed Threat Model

We also consider...

- Humans make decisions regarding their security based on the evaluation of the threat level they are subject to:
  - Humans had to decide whether to engage into attacks to become hunters or keep a way of life of gatherers;
  - Inherent faculty of human nature;

Proposed Threat Model

We also consider...

- Humans make decisions regarding their security based on the evaluation of the threat level they are subject to:
  - Humans had to decide whether to engage into attacks to become hunters or keep a way of life of gatherers;
  - Inherent faculty of human nature;
  - Some attacks may be thwarted, but inherently this will attract the human nature.

Human Centred Threat Model

- Considering worst case is not always the best option since it degrades usability;

Human Centred Threat Model

- Considering worst case is not always the best option since it degrades usability;
- The threat model must be adaptive;

Human Centred 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;

Human Centred 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

How can we do it?

- We start from Dolev-Yao, and then we remove one or more capabilities from the attacker;

Proposed Threat Model

How can we do it?

- 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;

Proposed Threat Model

How can we do it?

- 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;

Proposed Threat Model

How can we do it?

- 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

- "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

- Eavesdrop

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate
- Atomic Break Down

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate
- Atomic Break Down
- Crypto

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate
- Atomic Break Down
- Crypto
- Block

Proposed Threat Model

Capabilities

- Eavesdrop
- Initiate
- Atomic Break Down
- Crypto
- Block
- Fabricate

Proposed Threat Model

Capabilities

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

Proposed Threat Model

Capabilities

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

Proposed Threat Model

Capabilities

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

Some of the characteristics are achieved by the combination of our definitions (e.g. Replaying = Eavesdrop + Initiate)

Proposed Threat Model

Capabilities

- 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

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.
    - If the digits are equal, the pairing is successful

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 decode all the messages.

Example scenario: Bluetooth Pairing Protocol

Attacks

- 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) – Numeric Comparison

Ceremony

Protocol

$$
\begin{array}{lcccl}
\text{M1.} & B & \xrightarrow[DD]{} & A & : \; C_b = f1(pk_B, pk_A, N_b, 0) \\
\text{M2.} & A & \xrightarrow[DD]{} & B & : \; N_a \\
\text{M3.} & B & \xrightarrow[DD]{} & A & : \; N_b
\end{array}
$$

Assumptions

$$
\begin{array}{lcccl}
\text{M4.} & A & \xrightarrow[HD]{} & U_A & : \; V_a = g(pk_A, pk_B, N_a, N_b) \\
\text{M5.} & B & \xrightarrow[HD]{} & U_B & : \; V_b = g(pk_A, pk_B, N_a, N_b)
\end{array}
$$

$$
\begin{array}{lcccl}
\text{M6.} & U_A & \xrightarrow[HH]{} & U_B & : \; V_a \\
\text{M7.} & U_B & \xrightarrow[HH]{} & U_A & : \; V_b
\end{array}
$$

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_a or V_b and U_B from learning V_b or V_a, forcing them to learn V_i instead.

$$\frac{M_{1\ldots 7} \cup DY}{\begin{array}{r} V_a \wedge V_b \wedge V_i \in knows(I) \wedge \\ V_a \notin knows(A) \wedge V_b \notin knows(A) \wedge \\ V_b \notin knows(B) \wedge V_a \notin knows(B) \wedge \\ V_i \in knows(U_A) \wedge V_i \in knows(U_B) \end{array}}$$

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:

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

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.

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

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:

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

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 that it 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
- This kind of ceremony potentially trains users to detect different threat models

Where to go now?

- Specification of the threat model using an abstract verification method
- Automation for testing and design of security ceremonies
- Refining model to cope with more channels
- Redefining new ceremonies for old problems.

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.

Concluding Remarks

- The use of a worst-case scenario threat model is justifiable in security protocol scenarios;

Concluding Remarks

- The use of a worst-case scenario threat model is justifiable in security protocol scenarios;
- However, the same cannot be said for a human centric approach;

Concluding Remarks

- The use of a worst-case scenario threat model is justifiable in security protocol scenarios;
- However, the same cannot be said for a human centric approach;
- Human agents executing security ceremonies are constrained by the laws of physics and usual capabilities expected from human beings;

Concluding Remarks

- The use of a worst-case scenario threat model is justifiable in security protocol scenarios;
- However, the same cannot be said for a human centric approach;
- 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.

Discussion

- How do you relate the ideas of ceremonies to threat models?

Discussion

- How do you relate the ideas of ceremonies to threat models?
- Is it reasonable to use this threat model for security protocols?

Discussion

- How do you relate the ideas of ceremonies to threat models?
- Is it reasonable to use this threat model for security protocols?
- Can you describe a situation where you could gain leverage by using this threat model?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA