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

August-November 2016

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

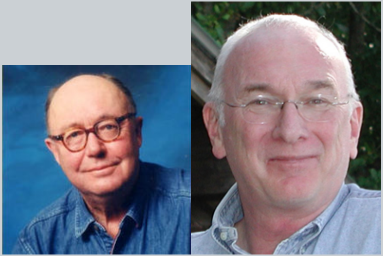
Historical facts

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

Introduction

Historical facts

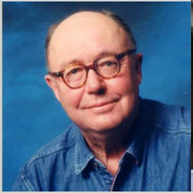
- Needham and Schroeder introduced the idea of an active attacker in 1978 who could:



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;

Introduction

Historical facts

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

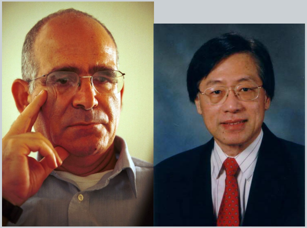
Introduction

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

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:

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;

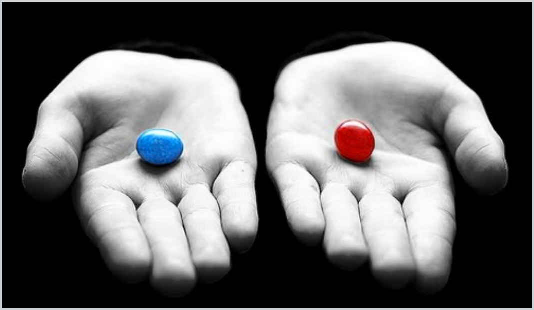
Introduction

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

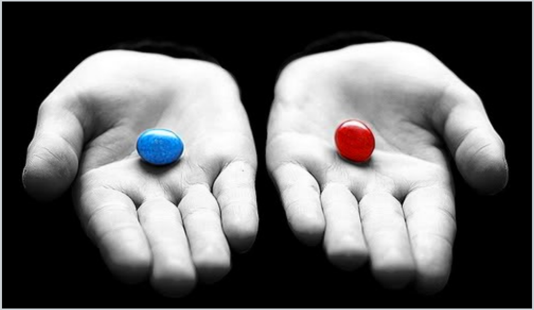
How do we sort this out?



- Clearly we have at least two choices:

Introduction

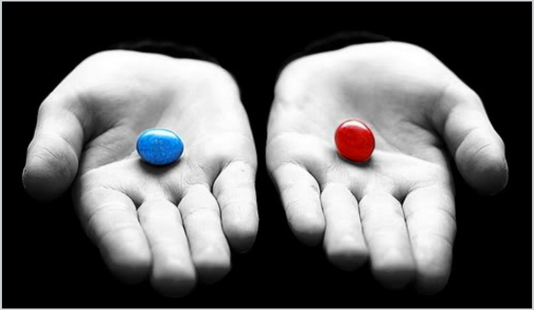
How do we sort this out?



- 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?

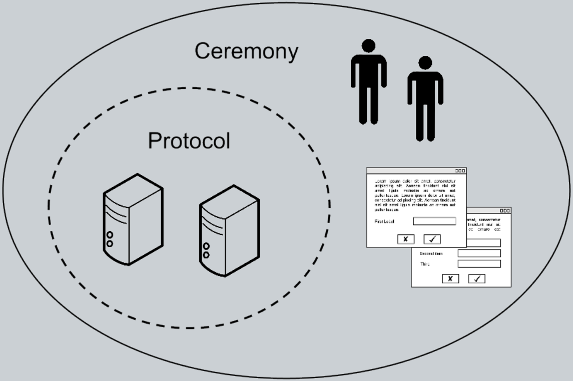
- User interaction is per se unpredictable;
- Modelling the user is very hard;
- Constructing a tool for that is complicated;
- The user is not part of the problem, but part of the solution!

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"



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

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
- 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;

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

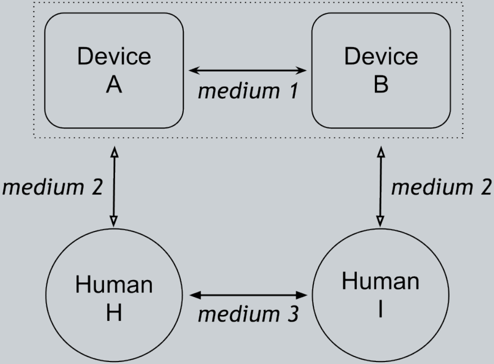
Scenario

- 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

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)

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