Threat Modelling for Symbolic Evaluation Dolev-Yao

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

How to Start!

- How can we tell if a cryptographic protocol or a security ceremony is secure?

How to Start!

- How can we tell if a cryptographic protocol or a security ceremony is secure?
- Phrased another way, how can we be sure that a given protocol/ceremony meets a given security goal?

How to Start!

- How can we tell if a cryptographic protocol or a security ceremony is secure?
- Phrased another way, how can we be sure that a given protocol/ceremony meets a given security goal?
- Whom are we defending against?

Notes about Security

- The sense of security is directly related to the threats available within the environment;

Notes about Security

- The sense of security is directly related to the threats available within the environment;
- One would feel unsafe in a setting where others would feel secure;

Notes about Security

- The sense of security is directly related to the threats available within the environment;
- One would feel unsafe in a setting where others would feel secure;
- Is security a sensation?

Notes about Insecurity

- As the security is related to the threats:

Notes about Insecurity

- As the security is related to the threats:
    - Assume no threats and you will be secure!

Notes about Insecurity

- As the security is related to the threats:
  - Assume no threats and you will be secure!
  - Assume weaker threats and you still be secure;

Notes about Insecurity

- As the security is related to the threats:
  - Assume no threats and you will be secure!
  - Assume weaker threats and you still be secure;
  - Are we able to foresee all the threats in a scenario?

Security and Insecurity comparison

- We can have two different things, one that we consider secure and another that we don't;

Security and Insecurity comparison

- We can have two different things, one that we consider secure and another that we don't;
- How do we compare two different things in terms of security?

Security and Insecurity comparison

- We can have two different things, one that we consider secure and another that we don't;
- How do we compare two different things in terms of security?
- We need a baseline for comparison;

Security and Insecurity comparison

- We can have two different things, one that we consider secure and another that we don't;
- How do we compare two different things in terms of security?
- We need a baseline for comparison;
- The name of this baseline is a Threat Model.

Changing the Baseline Matters

- We can recall the NSPKP example:
  - Needham and Schroeder assumed no internal could be an attacker;

Changing the Baseline Matters

- We can recall the NSPKP example:
  - Needham and Schroeder assumed no internal could be an attacker;
  - Everything worked for 15 years;

Changing the Baseline Matters

- We can recall the NSPKP example:
  - Needham and Schroeder assumed no internal could be an attacker;
  - Everything worked for 15 years;
  - Gavin Lowe assumed an internal could engage in the protocol to take advantage;

Changing the Baseline Matters

- We can recall the NSPKP example:
  - Needham and Schroeder assumed no internal could be an attacker;
  - Everything worked for 15 years;
  - Gavin Lowe assumed an internal could engage in the protocol to take advantage;
  - The protocol is considered broken since.

Importance of Threat Models

Lesson from NSSPK

To claim security and not to be surprised in the future you need to clearly specify the threat model of your protocol or ceremony and it must be as close as the environment where the protocol or ceremony will run within.

The Dolev-Yao Threat Model

- D. Dolev and A. Yao. "On the security of public key protocols". IEEE Transactions on Information Theory, 29(2):198-208. 1983;

The Dolev-Yao Threat Model

- D. Dolev and A. Yao. "On the security of public key protocols". IEEE Transactions on Information Theory, 29(2):198-208. 1983;
- The original motivation for the paper was to verify public key protocols against active attackers with considerable power;

The Dolev-Yao Threat Model

- D. Dolev and A. Yao. "On the security of public key protocols". IEEE Transactions on Information Theory, 29(2):198-208. 1983;
- The original motivation for the paper was to verify public key protocols against active attackers with considerable power;
- The setting for the paper was the cold war times;

The Dolev-Yao Threat Model

- D. Dolev and A. Yao. “On the security of public key protocols”. IEEE Transactions on Information Theory, 29(2):198-208. 1983;
- The original motivation for the paper was to verify public key protocols against active attackers with considerable power;
- The setting for the paper was the cold war times;
- Most mechanised formal methods for security analysis use some version of this model.

The Dolev-Yao Assumptions

- The underlying public key system is 'perfectly secure':

The Dolev-Yao Assumptions

- The underlying public key system is 'perfectly secure':
  - One-way functions are unbreakable;

The Dolev-Yao Assumptions

- The underlying public key system is 'perfectly secure':
  - One-way functions are unbreakable;
  - Public directory is secure and cannot be tampered with;

The Dolev-Yao Assumptions

- The underlying public key system is 'perfectly secure':
  - One-way functions are unbreakable;
  - Public directory is secure and cannot be tampered with;
  - Everyone has access to all public keys;

The Dolev-Yao Assumptions

- The underlying public key system is 'perfectly secure':
  - One-way functions are unbreakable;
  - Public directory is secure and cannot be tampered with;
  - Everyone has access to all public keys;
  - Only the peer knows his private key.

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:
  - He acts as a legitimate user;

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:
  - He acts as a legitimate user;
  - He can obtain any message from any party;

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:
  - He acts as a legitimate user;
  - He can obtain any message from any party;
  - He can initiate the protocol with any party, and can be a receiver to any party in the network;

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:
  - He acts as a legitimate user;
  - He can obtain any message from any party;
  - He can initiate the protocol with any party, and can be a receiver to any party in the network;
  - Can read any message, decompose it into parts and re-assemble.

The Dolev-Yao Assumptions

- Adversary has complete control over the entire network:
    - He acts as a legitimate user;
    - He can obtain any message from any party;
    - He can initiate the protocol with any party, and can be a receiver to any party in the network;
    - Can read any message, decompose it into parts and re-assemble.

The Dolev-Yao Assumptions

- Concurrent executions of the protocol can occur;

The Dolev-Yao Assumptions

- Concurrent executions of the protocol can occur;
- The attacker cannot gain partial knowledge and perform statistical tests;

The Dolev-Yao Assumptions

- Concurrent executions of the protocol can occur;
- The attacker cannot gain partial knowledge and perform statistical tests;
- The attacker can decrypt if and only if he knows the correct key;

The Dolev-Yao Assumptions

- Concurrent executions of the protocol can occur;
- The attacker cannot gain partial knowledge and perform statistical tests;
- The attacker can decrypt if and only if he knows the correct key;
- We assumes that cryptographic functions have no special properties.

The Dolev-Yao Benefits

- The model has the following features, which can be viewed as either benefits or restrictions depending on what you are trying to do:

The Dolev-Yao Benefits

- The model has the following features, which can be viewed as either benefits or restrictions depending on what you are trying to do:
  - It is simple to describe protocols in this model;

The Dolev-Yao Benefits

- The model has the following features, which can be viewed as either benefits or restrictions depending on what you are trying to do:
    - It is simple to describe protocols in this model;
    - Adversary has unlimited power, so although this is a conservative approach this may not be realistic;

The Dolev-Yao Benefits

- The model has the following features, which can be viewed as either benefits or restrictions depending on what you are trying to do:
  - It is simple to describe protocols in this model;
  - Adversary has unlimited power, so although this is a conservative approach this may not be realistic;
  - Protocols have a 'black-box' nature, which means that linking individual protocols with others is extremely difficult. Dolev-Yao helps on that.

The Dolev-Yao Features

- Secrecy properties: Alice is given a message M as input, and starts exchanging messages with Bob, with the goal of sending message M to Bob in a secret way;

The Dolev-Yao Features

- Secrecy properties: Alice is given a message M as input, and starts exchanging messages with Bob, with the goal of sending message M to Bob in a secret way;
- The security property is that an adversary cannot recover M, even if actively interfering with the protocol;

The Dolev-Yao Features

- Secrecy properties: Alice is given a message M as input, and starts exchanging messages with Bob, with the goal of sending message M to Bob in a secret way;
- The security property is that an adversary cannot recover M, even if actively interfering with the protocol;
- No other security properties are considered.

The Dolev-Yao Features

- Stateless parties: The main limitation on the honest parties is that they are stateless;

The Dolev-Yao Features

- Stateless parties: The main limitation on the honest parties is that they are stateless;
- The messages transmitted by a party at every step of the protocol are a function of their initial knowledge and the message they just received;
- In particular, parties cannot use information collected from previous messages not addressed to them;
- For this reason, these protocols have been named "ping-pong" protocols;

The Dolev-Yao Features

- Stateless parties: The main limitation on the honest parties is that they are stateless;
- The messages transmitted by a party at every step of the protocol are a function of their initial knowledge and the message they just received;
- In particular, parties cannot use information collected from previous messages not addressed to them;
- For this reason, these protocols have been named ”ping-pong” protocols;
- We observe that the stateless restriction is only put on the honest parties, and the adversary can maintain state, record communications, and store values that are subsequently used in the construction of messages;

The Dolev-Yao Features

- Concurrent execution: The adversary can start an arbitrary number of protocol executions, involving different sets of parties, where each player can participate in several concurrent executions;

The Dolev-Yao Features

- Concurrent execution: The adversary can start an arbitrary number of protocol executions, involving different sets of parties, where each player can participate in several concurrent executions;
- In this respect, the model considered here is more general than the computational model considered at the time, which focused on single protocol execution;

The Dolev-Yao Features

- Concurrent execution: The adversary can start an arbitrary number of protocol executions, involving different sets of parties, where each player can participate in several concurrent executions;
- In this respect, the model considered here is more general than the computational model considered at the time, which focused on single protocol execution;
- The computational cryptography community started addressing the important issue of concurrency only in the 90's.

The Dolev-Yao Features

- In the Dolev-Yao model, there are two kinds of active parties: honest participants and the adversary;

The Dolev-Yao Features

- In the Dolev-Yao model, there are two kinds of active parties: honest participants and the adversary;
- The honest participants follow the steps of the protocol without deviation;

The Dolev-Yao Features

- In the Dolev-Yao model, there are two kinds of active parties: honest participants and the adversary;
- The honest participants follow the steps of the protocol without deviation;
- The attacker do not follow the rules;

The Dolev-Yao Features

- In the Dolev-Yao model, there are two kinds of active parties: honest participants and the adversary;
- The honest participants follow the steps of the protocol without deviation;
- The attacker do not follow the rules;
- The peers do not share long term secrets, even the attacker keeps things for himself.

Dolev-Yao in Practice

- All the peers start with some knowledge set, including all public information, peers names and their own random numbers to be used as nonces;

Dolev-Yao in Practice

- All the peers start with some knowledge set, including all public information, peers names and their own random numbers to be used as nonces;
- If a message is cast in the network, it go to the destination's knowledge set and the attackers knowledge set (Eavesdrop);

Dolev-Yao in Practice

- From the attacker knowledge set:
  - He can decrypt whatever he has the key to do so and re-encrypt whatever he know with the keys he has at hand (Encryption);

Dolev-Yao in Practice

- From the attacker knowledge set:
  - He can decrypt whatever he has the key to do so and re-encrypt whatever he know with the keys he has at hand (Encryption);
  - He can break down messages to atomic components (Atomic Breakdown);

Dolev-Yao in Practice

- From the attacker knowledge set:
  - He can decrypt whatever he has the key to do so and re-encrypt whatever he know with the keys he has at hand (Encryption);
  - He can break down messages to atomic components (Atomic Breakdown);
  - He can re-arrange all the components he knows in all possible ways to form new messages (Fabricate);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);
- He can replay any message he collects from traffic (Replay);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);
- He can replay any message he collects from traffic (Replay);
- He can prevent the delivery of any message (Block);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);
- He can replay any message he collects from traffic (Replay);
- He can prevent the delivery of any message (Block);
- He can engage legitimately with other peers on the protocol (Initiate);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);
- He can replay any message he collects from traffic (Replay);
- He can prevent the delivery of any message (Block);
- He can engage legitimately with other peers on the protocol (Initiate);
- He can re-arrange the order of the messages in traffic (Re-order);

Dolev-Yao in Practice

- He can modify messages in transit (Modify);
- He can replay any message he collects from traffic (Replay);
- He can prevent the delivery of any message (Block);
- He can engage legitimately with other peers on the protocol (Initiate);
- He can re-arrange the order of the messages in traffic (Re-order);
- He can mimic the identity of any peer in the network (Spoof).

Dolev-Yao Implementation

- It is usually logically implemented;

Dolev-Yao Implementation

- It is usually logically implemented;
- It uses free variables to allow for the powers to happen;

Dolev-Yao Implementation

- It is usually logically implemented;
- It uses free variables to allow for the powers to happen;
- Although the amount of knowledge the attacker can have is potentially unbound, it is finite;

Dolev-Yao Implementation

- It is usually logically implemented;
- It uses free variables to allow for the powers to happen;
- Although the amount of knowledge the attacker can have is potentially unbound, it is finite;
- Some techniques create other significant limits to the Dolev-Yao Threat Model.

Discussion

- Is Dolev-Yao enough to put a security protocols against and claim it secure?

Discussion

- Is Dolev-Yao enough to put a security protocols against and claim it secure?
- Can you foresee some capability missing?

Discussion

- Is Dolev-Yao enough to put a security protocols against and claim it secure?
- Can you foresee some capability missing?
- Is Dolev-Yao sufficient to compare two security protocols?

Discussion

- Is Dolev-Yao enough to put a security protocols against and claim it secure?
- Can you foresee some capability missing?
- Is Dolev-Yao sufficient to compare two security protocols?
- What can go wrong when we compare two security protocols that use Dolev-Yao as Threat Model

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA