Threat Modelling 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

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

- 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 assume 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;

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;

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 does 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 does 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 knows 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 knows 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 knows 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?

Dolev-Yao Considerations

- DY can be considered the standard threat model to study security protocols;

Dolev-Yao Considerations

- DY can be considered the standard threat model to study security protocols;.
- The DY attacker controls the entire network although he cannot perform cryptanalysis;

Dolev-Yao Considerations

- DY can be considered the standard threat model to study security protocols;.
- The DY attacker controls the entire network although he cannot perform cryptanalysis;
- The DY model has remarkably favoured the discovery of significant protocol flaws, but the attacker has significantly changed today;

Dolev-Yao Considerations

- DY can be considered the standard threat model to study security protocols;.
- The DY attacker controls the entire network although he cannot perform cryptanalysis;
- The DY model has remarkably favoured the discovery of significant protocol flaws, but the attacker has significantly changed today;
- To become an attacker has never been so easy.

A Family of Variations for Dolev-Yao

- B.U.G;

A Family of Variations for Dolev-Yao

- B.U.G;
- The Rational Attacker;

A Family of Variations for Dolev-Yao

- B.U.G;
- The Rational Attacker;
- The General Attacker;

A Family of Variations for Dolev-Yao

- B.U.G;
- The Rational Attacker;
- The General Attacker;
- Multi Attacker;

A Family of Variations for Dolev-Yao

- B.U.G;
- The Rational Attacker;
- The General Attacker;
- Multi Attacker;
- Distributed Attacker.

The B.U.G Threat Model

- B.U.G. dates back to 2002;

The B.U.G Threat Model

- B.U.G. dates back to 2002;
- The name is a permuted acronym for the “Good”, the “Bad” and the “Ugly”;

The B.U.G Threat Model

- B.U.G. dates back to 2002;
- The name is a permuted acronym for the “Good”, the “Bad” and the “Ugly”;
- This model attempts stricter adherence to reality by partitioning the participants into three groups;

The B.U.G Threat Model

- B.U.G. dates back to 2002;
- The name is a permuted acronym for the “Good”, the “Bad” and the “Ugly”;
- This model attempts stricter adherence to reality by partitioning the participants into three groups;
- The Good principals would follow the protocol;

The B.U.G Threat Model

- B.U.G. dates back to 2002;
- The name is a permuted acronym for the “Good”, the “Bad” and the “Ugly”;
- This model attempts stricter adherence to reality by partitioning the participants into three groups;
- The Good principals would follow the protocol;
- The Bad would in addition try to subvert it;

The B.U.G Threat Model

- B.U.G. dates back to 2002;
- The name is a permuted acronym for the "Good", the "Bad" and the "Ugly";
- This model attempts stricter adherence to reality by partitioning the participants into three groups;
- The Good principals would follow the protocol;
- The Bad would in addition try to subvert it;
- The Ugly would be ready to either behaviour.

The B.U.G Threat Model Insights

- A principal may change role and decide to attempt illegal exploitation of a protocol although he has always conformed to it so far;

The B.U.G Threat Model Insights

- A principal may change role and decide to attempt illegal exploitation of a protocol although he has always conformed to it so far;
- It changes the idea of a single attacker since anyone could attack;

The B.U.G Threat Model Insights

- A principal may change role and decide to attempt illegal exploitation of a protocol although he has always conformed to it so far;
- It changes the idea of a single attacker since anyone could attack;
- The principle behind this threat model is that the attackers do not share long term secrets.

The B.U.G Threat Model Issues

- It is unclear on how dynamic updates should be on the behaviour:

The B.U.G Threat Model Issues

- It is unclear on how dynamic updates should be on the behaviour:
    - One could change behaviour after every single message;

The B.U.G Threat Model Issues

- It is unclear on how dynamic updates should be on the behaviour:
  - One could change behaviour after every single message;
  - Either sent, received or cast;

The B.U.G Threat Model Issues

- It is unclear on how dynamic updates should be on the behaviour:
  - One could change behaviour after every single message;
  - Either sent, received or cast;
- This complicates a lot the mechanisations of the attacker, because all behaviour is possible.

The Rational Attacker Threat Model

- BUG appeared overly detailed, and was simplified as The Rational Attacker Threat Model;

The Rational Attacker Threat Model

- BUG appeared overly detailed, and was simplified as The Rational Attacker Threat Model;
- It was conceived in 2008;

The Rational Attacker Threat Model

- BUG appeared overly detailed, and was simplified as The Rational Attacker Threat Model;
- It was conceived in 2008;
- The Rational Attacker let any principal make cost/benefit decisions at any time to either behave according to the protocol or not;

The Rational Attacker Threat Model

- BUG appeared overly detailed, and was simplified as The Rational Attacker Threat Model;
- It was conceived in 2008;
- The Rational Attacker let any principal make cost/benefit decisions at any time to either behave according to the protocol or not;
- Analysing a protocol under the Rational Attacker requires specifying each principal's cost and benefit functions.

The Rational Attacker Insights

- The Rational Attacker seems out of reach for the current mechanised approaches, especially for bound verification techniques;

The Rational Attacker Insights

- The Rational Attacker seems out of reach for the current mechanised approaches, especially for bound verification techniques;
- Although complex to mechanise, the Rational Attacker is more realistic than B.U.G.;

The Rational Attacker Insights

- The Rational Attacker seems out of reach for the current mechanised approaches, especially for bound verification techniques;
- Although complex to mechanise, the Rational Attacker is more realistic than B.U.G.;
- In the wild, it is common to the attacker to make cost/benefit analysis when to engage or not;

The Rational Attacker Insights

- The Rational Attacker seems out of reach for the current mechanised approaches, especially for bound verification techniques;
- Although complex to mechanise, the Rational Attacker is more realistic than B.U.G.;
- In the wild, it is common to the attacker to make cost/benefit analysis when to engage or not;
- The Rational Attacker bring all game theory into the protocols' scenarios.

The Rational Attacker Issues

- The Rational Attacker is not clear whether the cost/benefit function is fixed or variable;

The Rational Attacker Issues

- The Rational Attacker is not clear whether the cost/benefit function is fixed or variable;
- One would argue that the objectives of the attacker are not static and that it would change depending on the gains made so far;

The Rational Attacker Issues

- The Rational Attacker is not clear whether the cost/benefit function is fixed or variable;
- One would argue that the objectives of the attacker are not static and that it would change depending on the gains made so far;
- Mechanisation is not only and issue of representativeness of the formal verification technique, but an entangled problem.

The General Attacker Threat Model

- The General Attacker abstracts away the actual cost/benefit analysis in a simplified model;

The General Attacker Threat Model

- The General Attacker abstracts away the actual cost/benefit analysis in a simplified model;
- Any principal may behave as a Dolev-Yao attacker;

The General Attacker Threat Model

- The General Attacker abstracts away the actual cost/benefit analysis in a simplified model;
- Any principal may behave as a Dolev-Yao attacker;
- The change of perspective in RA or in GA with respect to DY is clear: principals do not collude for a common aim but, rather, each of them acts for his own personal sake;

The General Attacker Threat Model

- The General Attacker abstracts away the actual cost/benefit analysis in a simplified model;
- Any principal may behave as a Dolev-Yao attacker;
- The change of perspective in RA or in GA with respect to DY is clear: principals do not collude for a common aim but, rather, each of them acts for his own personal sake;
- By contrast, a pair of colluding DY attackers is equivalent to a single DY attacker in terms of generated attacks;

The General Attacker Threat Model

- The General Attacker abstracts away the actual cost/benefit analysis in a simplified model;
- Any principal may behave as a Dolev-Yao attacker;
- The change of perspective in RA or in GA with respect to DY is clear: principals do not collude for a common aim but, rather, each of them acts for his own personal sake;
- By contrast, a pair of colluding DY attackers is equivalent to a single DY attacker in terms of generated attacks;
    - This is confirmed by a formal proof.

The General Attacker Insights

- Endowing each principal with the entire potential of a DY attacker signifies that he may send any of the messages he can form to anyone;

The General Attacker Insights

- Endowing each principal with the entire potential of a DY attacker signifies that he may send any of the messages he can form to anyone;
- Such messages include both the legal ones, conforming to the protocol in use, and the illegal, forged ones, which he can build from the analysis of the traffic though without cryptanalysis.

The General Attacker Issues

- It was suggested that the General Attacker is similar to Dolev-Yao provided that all principals reveal their secrets to the attacker (Augmented Dolev-Yao);

The General Attacker Issues

- It was suggested that the General Attacker is similar to Dolev-Yao provided that all principals reveal their secrets to the attacker (Augmented Dolev-Yao);
- They appear equivalent:

The General Attacker Issues

- It was suggested that the General Attacker is similar to Dolev-Yao provided that all principals reveal their secrets to the attacker (Augmented Dolev-Yao);
- They appear equivalent:
    - Any illegal message that a principal may send in General Attacker may be sent by the single augmented Dolev-Yao attacker;

The General Attacker Issues

- It was suggested that the General Attacker is similar to Dolev-Yao provided that all principals reveal their secrets to the attacker (Augmented Dolev-Yao);
- They appear equivalent:
  - Any illegal message that a principal may send in General Attacker may be sent by the single augmented Dolev-Yao attacker;
  - This happens because he knows everyone's secrets.

The General Attacker versus Augmented Dolev-Yao

- Augmented Dolev-Yao entangles the interpretation of attacks where principals attack each other;

The General Attacker versus Augmented Dolev-Yao

- Augmented Dolev-Yao entangles the interpretation of attacks where principals attack each other;
- The single attacker will always be the originator of any attack, complicating the identification of the real perpetrator;

The General Attacker versus Augmented Dolev-Yao

- Augmented Dolev-Yao entangles the interpretation of attacks where principals attack each other;
- The single attacker will always be the originator of any attack, complicating the identification of the real perpetrator;
- For attacks against the attacker, the model will feature the attacker attacking himself, thus stretching the interpretation of the victim to an extreme;

The General Attacker versus Augmented Dolev-Yao

- Augmented Dolev-Yao entangles the interpretation of attacks where principals attack each other;
- The single attacker will always be the originator of any attack, complicating the identification of the real perpetrator;
- For attacks against the attacker, the model will feature the attacker attacking himself, thus stretching the interpretation of the victim to an extreme;
- Perpetrator and victim are naturally expressed in GA because its gist is exactly to reflect modern everyone-for-themselves scenarios.

The Multi Attacker Threat Model

- In the Multi Attacker each principal may behave as a Dolev-Yao attacker but will never reveal his long-term secrets;

The Multi Attacker Threat Model

- In the Multi Attacker each principal may behave as a Dolev-Yao attacker but will never reveal his long-term secrets;
- It was conceived in 2011;

The Multi Attacker Threat Model

- In the Multi Attacker each principal may behave as a Dolev-Yao attacker but will never reveal his long-term secrets;
- It was conceived in 2011;
- Multi Attacker can be seen as a refinement of General Attacker with some rationality that avoids the trivial impersonation attacks;

The Multi Attacker Threat Model

- In the Multi Attacker each principal may behave as a Dolev-Yao attacker but will never reveal his long-term secrets;
- It was conceived in 2011;
- Multi Attacker can be seen as a refinement of General Attacker with some rationality that avoids the trivial impersonation attacks;
- It helps to understand some new types of attacks.

The Multi Attacker Insights

- Analysing protocols under the Multi Attacker threat model yields unknown scenarios of retaliation or anticipation;

The Multi Attacker Insights

- Analysing protocols under the Multi Attacker threat model yields unknown scenarios of retaliation or anticipation;
- If an attack can be retaliated under Multi Attacker, such a scenario will not occur under Rational Attacker because the cost of attacking clearly overdoes its benefit, and hence the attacker will not attack in the first place;

The Multi Attacker Insights

- Analysing protocols under the Multi Attacker threat model yields unknown scenarios of retaliation or anticipation;
- If an attack can be retaliated under Multi Attacker, such a scenario will not occur under Rational Attacker because the cost of attacking clearly overdoes its benefit, and hence the attacker will not attack in the first place;
- This changes the game of how a powerful attacker would attack, because retaliation may let the attacker vulnerable.

The Multi Attacker Issues

- The Multi Attacker do not use its full capabilities to derive partial information;

The Multi Attacker Issues

- The Multi Attacker do not use its full capabilities to derive partial information;
- By being powerful and knowing what is going on, he could anticipate what other Multi Attacker have on their knowledge set;

The Multi Attacker Issues

- The Multi Attacker do not use its full capabilities to derive partial information;
- By being powerful and knowing what is going on, he could anticipate what other Multi Attacker have on their knowledge set;
- This is not encoded on the attacker;

The Multi Attacker Issues

- The Multi Attacker do not use its full capabilities to derive partial information;
- By being powerful and knowing what is going on, he could anticipate what other Multi Attacker have on their knowledge set;
- This is not encoded on the attacker;
- This would make competition between the attacker fiercer.

The Distributed Attacker Threat Model

- The Distributed Attacker is an evolution of the Multi Attacker where the principals can have different powers;

The Distributed Attacker Threat Model

- The Distributed Attacker is an evolution of the Multi Attacker where the principals can have different powers;
- It was conceived in 2015;

The Distributed Attacker Threat Model

- The Distributed Attacker is an evolution of the Multi Attacker where the principals can have different powers;
- It was conceived in 2015;
- It was tailored for a layered strategy for security ceremonies;

The Distributed Attacker Threat Model

- The Distributed Attacker is an evolution of the Multi Attacker where the principals can have different powers;
- It was conceived in 2015;
- It was tailored for a layered strategy for security ceremonies;
- It is reasonable to use in protocol verification because the real capabilities of the multi-attacker we have are not clear and eventually will not be the same.

The Distributed Attacker Insights

- It is based on Martina-Carlos ideas of breaking down the power of the Dolev-Yao attacker;

The Distributed Attacker Insights

- It is based on Martina-Carlos ideas of breaking down the power of the Dolev-Yao attacker;
- Acknowledging that each multi-attacker has different powers it a good strategy that can show us the competition between the attacker for the target;

The Distributed Attacker Insights

- It is based on Martina-Carlos ideas of breaking down the power of the Dolev-Yao attacker;
- Acknowledging that each multi-attacker has different powers it a good strategy that can show us the competition between the attacker for the target;
- It was shown that we can mechanise such attacker using First-Order Logics;

The Distributed Attacker Insights

- It is based on Martina-Carlos ideas of breaking down the power of the Dolev-Yao attacker;
- Acknowledging that each multi-attacker has different powers it a good strategy that can show us the competition between the attacker for the target;
- It was shown that we can mechanise such attacker using First-Order Logics;
- No issues were brought so far due to its freshness within the protocol and ceremony verification communities.

Discussion

- Can you identify a protocol where using one of this evolutions of Dolev-Yao can bring insights of new attacks?

Discussion

- Can you identify a protocol where using one of this evolutions of Dolev-Yao can bring insights of new attacks?
- Which one would make more sense today?

Discussion

- Can you identify a protocol where using one of this evolutions of Dolev-Yao can bring insights of new attacks?
- Which one would make more sense today?
- Choosing one Threat Model to work invalidate the others?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA