B.U.G. Threat Model Family

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

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 we 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