Advanced Security Properties and Properties Composition

Design and Verification of Security Protocols and Security Ceremonies

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

August-November 2016

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Disclaimer

Disclaimer!

What we will see in the next slides is not a precise scientific description of the properties, but a basis for exemplification of what is out there just to foster discussion.

Disclaimer

Disclaimer!

What we will see in the next slides is not a precise scientific description of the properties, but a basis for exemplification of what is out there just to foster discussion.

- We will be seeing common security properties that happen on literature;

Disclaimer

Disclaimer!

What we will see in the next slides is not a precise scientific description of the properties, but a basis for exemplification of what is out there just to foster discussion.

- We will be seeing common security properties that happen on literature;
- The descriptions are solely the lecturer's opinion on the properties and may be wrong.

List of Advanced Security Properties

- Forward secrecy;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;
- Receipt-freeness;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;
- Receipt-freeness;
- Coercion-resistance;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;
- Receipt-freeness;
- Coercion-resistance;
- Privacy;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;
- Receipt-freeness;
- Coercion-resistance;
- Privacy;
- Anonymity;

List of Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Plausible Deniability;
- Availability;
- Eligibility;
- Fairness;
- Receipt-freeness;
- Coercion-resistance;
- Privacy;
- Anonymity;
- Transparency.

Forward Secrecy

- Forward secrecy relates to the non-interference of short term keys leakage to new short term keys;

Forward Secrecy

- Forward secrecy relates to the non-interference of short term keys leakage to new short term keys;
- It does not relate to long term keys;

Forward Secrecy

- Forward secrecy relates to the non-interference of short term keys leakage to new short term keys;
- It does not relate to long term keys;
- Is usually obtained by the negotiation of short term keys only based on long term keys;

Forward Secrecy

- Forward secrecy relates to the non-interference of short term keys leakage to new short term keys;
- It does not relate to long term keys;
- Is usually obtained by the negotiation of short term keys only based on long term keys;
- Has a complementary property that is Backwards secrecy;

Forward Secrecy

- Forward secrecy relates to the non-interference of short term keys leakage to new short term keys;
- It does not relate to long term keys;
- Is usually obtained by the negotiation of short term keys only based on long term keys;
- Has a complementary property that is Backwards secrecy;
- Having both lead to full non-interference among session keys.

Non-repudiation

- Is the inability to deny knowledge of a message;

Non-repudiation

- Is the inability to deny knowledge of a message;
- Happens as non-repudiation of origin, meaning authorship;

Non-repudiation

- Is the inability to deny knowledge of a message;
- Happens as non-repudiation of origin, meaning authorship;
- Happens as non-repudiation of destiny, meaning confirmation of reception;

Non-repudiation

- Is the inability to deny knowledge of a message;
- Happens as non-repudiation of origin, meaning authorship;
- Happens as non-repudiation of destiny, meaning confirmation of reception;
- Is usually implemented using asymmetric crypto in digital signature mode;

Non-repudiation

- Is the inability to deny knowledge of a message;
- Happens as non-repudiation of origin, meaning authorship;
- Happens as non-repudiation of destiny, meaning confirmation of reception;
- Is usually implemented using asymmetric crypto in digital signature mode;
- Can also be achieve by the use of commitments.

Plausible Deniability

- Is the ability to deny knowledge of a message;

Plausible Deniability

- Is the ability to deny knowledge of a message;
- Act the the courter property of Non-Repudiation;

Plausible Deniability

- Is the ability to deny knowledge of a message;
- Act the the courter property of Non-Repudiation;
- Is implemented shared secret crypto;

Plausible Deniability

- Is the ability to deny knowledge of a message;
- Act the the courter property of Non-Repudiation;
- Is implemented shared secret crypto;
- Can also happen on origin, destination or both.

Availability

- Is the property that relates to presence of knowledge whenever needed;

Availability

- Is the property that relates to presence of knowledge whenever needed;
- Is difficult to reach by crypto-means;

Availability

- Is the property that relates to presence of knowledge whenever needed;
- Is difficult to reach by crypto-means;
- Is usually reached using replication;

Availability

- Is the property that relates to presence of knowledge whenever needed;
- Is difficult to reach by crypto-means;
- Is usually reached using replication;
- There are some interesting primitives that achieve availability such as secret-sharing.

Eligibility

- Is the property that states authority to a peer to act;

Eligibility

- Is the property that states authority to a peer to act;
- Usually present on election protocols;

Eligibility

- Is the property that states authority to a peer to act;
- Usually present on election protocols;
- Is related and derived from Authentication;

Eligibility

- Is the property that states authority to a peer to act;
- Usually present on election protocols;
- Is related and derived from Authentication;
- Can also happen through delegation;

Eligibility

- Is the property that states authority to a peer to act;
- Usually present on election protocols;
- Is related and derived from Authentication;
- Can also happen through delegation;
- Is implemented in this later case by the usage of tickets;

Eligibility

- Is the property that states authority to a peer to act;
- Usually present on election protocols;
- Is related and derived from Authentication;
- Can also happen through delegation;
- Is implemented in this later case by the usage of tickets;
- Can also control the number of times the peer is allowed to do something.

Fairness

- Fairness is the properties that guarantees that no information is acquired out of the right time;

Fairness

- Fairness is the properties that guarantees that no information is acquired out of the right time;
- In election protocols it means that no early results can be obtained which could influence the remaining voters;

Fairness

- Fairness is the properties that guarantees that no information is acquired out of the right time;
- In election protocols it means that no early results can be obtained which could influence the remaining voters;
- Is usually implemented with encryption (either symmetric or asymmetric);

Fairness

- Fairness is the properties that guarantees that no information is acquired out of the right time;
- In election protocols it means that no early results can be obtained which could influence the remaining voters;
- Is usually implemented with encryption (either symmetric or asymmetric);
- The keys are them distributed is such a way that only an agreement can enable decryption.

Receipt-freeness

- Receipt-freeness is the property that the peer does not carry any proof of acts within the protocol;

Receipt-freeness

- Receipt-freeness is the property that the peer does not carry any proof of acts within the protocol;
- In election protocols it means that a voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way;

Receipt-freeness

- Receipt-freeness is the property that the peer does not carry any proof of acts within the protocol;
- In election protocols it means that a voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way;
- It is tricky to achieve when combined with other properties;

Receipt-freeness

- Receipt-freeness is the property that the peer does not carry any proof of acts within the protocol;
- In election protocols it means that a voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way;
- It is tricky to achieve when combined with other properties;
- Implementation usually is not done using cryptographic means.

Coercion-resistance

- Coercion-resistance is the property that avoid a peer to act in certain way against its own will and forced by an external entity;

Coercion-resistance

- Coercion-resistance is the property that avoid a peer to act in certain way against its own will and forced by an external entity;
- In election protocols it means that a voter cannot cooperate with a coercer to prove to him that she voted in a certain way;

Coercion-resistance

- Coercion-resistance is the property that avoid a peer to act in certain way against its own will and forced by an external entity;
- In election protocols it means that a voter cannot cooperate with a coercer to prove to him that she voted in a certain way;
- It is usually achieve by using the last commitment within the protocol;

Coercion-resistance

- Coercion-resistance is the property that avoid a peer to act in certain way against its own will and forced by an external entity;
- In election protocols it means that a voter cannot cooperate with a coercer to prove to him that she voted in a certain way;
- It is usually achieve by using the last commitment within the protocol;
- Implementation usually depends of Receipt-freeness but is not a requirement.

Verifiability

- Is the property that allows for peers to be assured that their interaction was perceived within the protocol;

Verifiability

- Is the property that allows for peers to be assured that their interaction was perceived within the protocol;
- Is usually implemented using bulletin boards;

Verifiability

- Is the property that allows for peers to be assured that their interaction was perceived within the protocol;
- Is usually implemented using bulletin boards;
- In election protocols it can be specialised in:

Verifiability

- Is the property that allows for peers to be assured that their interaction was perceived within the protocol;
- Is usually implemented using bulletin boards;
- In election protocols it can be specialised in:
  - Individual verifiability: a voter can verify that her vote was really counted;

Verifiability

- Is the property that allows for peers to be assured that their interaction was perceived within the protocol;
- Is usually implemented using bulletin boards;
- In election protocols it can be specialised in:
  - Individual verifiability: a voter can verify that her vote was really counted;
  - Universal verifiability: the published outcome really is the sum of all the votes.

Privacy

- Privacy is the property that allows for peers to choose the amount of data that is being release to other peers;

Privacy

- Privacy is the property that allows for peers to choose the amount of data that is being release to other peers;
- Has a controversial definition since it is related to a personal feeling;

Privacy

- Privacy is the property that allows for peers to choose the amount of data that is being release to other peers;
- Has a controversial definition since it is related to a personal feeling;
- It is intrinsically related to Confidentiality;

Privacy

- Privacy is the property that allows for peers to choose the amount of data that is being release to other peers;
- Has a controversial definition since it is related to a personal feeling;
- It is intrinsically related to Confidentiality;
- In election protocols it means that the system cannot reveal how a particular voter voted;

Privacy

- Privacy is the property that allows for peers to choose the amount of data that is being release to other peers;
- Has a controversial definition since it is related to a personal feeling;
- It is intrinsically related to Confidentiality;
- In election protocols it means that the system cannot reveal how a particular voter voted;

Anonymity

- Anonymity is the property that does not allow identification of peers;

Anonymity

- Anonymity is the property that does not allow identification of peers;
- Is usually achieve by using obfuscation techniques;

Anonymity

- Anonymity is the property that does not allow identification of peers;
- Is usually achieve by using obfuscation techniques;
- Usually is implemented with hashes or MACs;

Anonymity

- Anonymity is the property that does not allow identification of peers;
- Is usually achieve by using obfuscation techniques;
- Usually is implemented with hashes or MACs;
- Is a form of plausible deniability.

Transparency

- Transparency can be defined the distance of a message from ground truth;

Transparency

- Transparency can be defined the distance of a message from ground truth;
- It a very new property that is actually being studied still;

Transparency

- Transparency can be defined the distance of a message from ground truth;
- It a very new property that is actually being studied still;
- Is present in crypto-currency protocols and in health related systems;

Transparency

- Transparency can be defined the distance of a message from ground truth;
- It a very new property that is actually being studied still;
- Is present in crypto-currency protocols and in health related systems;
- Is a dichotomy of Privacy.

Discussion

- Which other properties did you hear about?

Discussion

- Which other properties did you hear about?
- Which are the dichotomies you can see between the properties shown today?

Discussion

- Which other properties did you hear about?
- Which are the dichotomies you can see between the properties shown today?
- Can you foresee an online activity that you require a property not listed here?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA