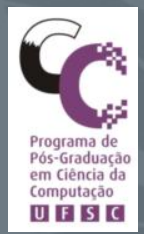
Security Properties, Advanced Security Properties and Properties Composition

Design and Verification of Security Protocols and Security Ceremonies

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

March-June 2018



UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Security Protocols

- The focus of security protocols is on secure communications;

Security Protocols

- The focus of security protocols is on secure communications;
- Two or more parties are involved;

Security Protocols

- The focus of security protocols is on secure communications;
- Two or more parties are involved;
- Communication is carried over an insecure network;

Security Protocols

- The focus of security protocols is on secure communications;
- Two or more parties are involved;
- Communication is carried over an insecure network;
- Cryptography is used to achieve some goal.

Security Protocols Goals

- Guided by user needs:

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;
  - Authenticate peers;

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;
  - Authenticate peers;
  - Enable secure money transfer;

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;
  - Authenticate peers;
  - Enable secure money transfer;
  - Provide anonymity;

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;
  - Authenticate peers;
  - Enable secure money transfer;
  - Provide anonymity;
  - Authenticate data;

Security Protocols Goals

- Guided by user needs:
  - Provide an end-to-end encryption channel;
  - Authenticate peers;
  - Enable secure money transfer;
  - Provide anonymity;
  - Authenticate data;
- Usually are a claim of designers that must be verified.

Building Blocks

- Symmetric cryptography;

Building Blocks

- Symmetric cryptography;
- Cryptographic hashes;

Building Blocks

- Symmetric cryptography;
- Cryptographic hashes;
- Asymmetric cryptography;

Building Blocks

- Symmetric cryptography;
- Cryptographic hashes;
- Asymmetric cryptography;
- Advanced primitives;

Building Blocks

- Symmetric cryptography;
- Cryptographic hashes;
- Asymmetric cryptography;
- Advanced primitives;
- Other security protocols;

Standard Security Properties

- Confidentiality;

Standard Security Properties

- Confidentiality;
- Integrity;

Standard Security Properties

- Confidentiality;
- Integrity;
- Timeliness;

Standard Security Properties

- Confidentiality;
- Integrity;
- Timeliness;
- Authentication.

Advanced Security Properties

- Forward secrecy;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Availability;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Availability;
- Anonymity rather than Authenticity;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Availability;
- Anonymity rather than Authenticity;
- Plausible Deniability rather than Non-Repudiation;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Availability;
- Anonymity rather than Authenticity;
- Plausible Deniability rather than Non-Repudiation;
- Transparency instead of Privacy;

Advanced Security Properties

- Forward secrecy;
- Non-repudiation;
- Availability;
- Anonymity rather than Authenticity;
- Plausible Deniability rather than Non-Repudiation;
- Transparency instead of Privacy;
- Etc...

Confidentiality

- Also called secrecy;

Confidentiality

- Also called secrecy;
- Is the usual main goal of cryptography;

Confidentiality

- Also called secrecy;
- Is the usual main goal of cryptography;
- Can be provided using symmetric cryptography or asymmetric cryptography;

Confidentiality

- Also called secrecy;
- Is the usual main goal of cryptography;
- Can be provided using symmetric cryptography or asymmetric cryptography;
- Symmetric cryptography is not “clean cut” since it always provide some sort of authentication;

Confidentiality

- Also called secrecy;
- Is the usual main goal of cryptography;
- Can be provided using symmetric cryptography or asymmetric cryptography;
- Symmetric cryptography is not “clean cut” since it always provide some sort of authentication;
- Asymmetric cryptography separate confidentiality from authentication.

Confidentiality Examples

- A sends to B message M encrypted with shared key Kab;

Confidentiality Examples

- A sends to B message M encrypted with shared key Kab;
- A sends to B message M encrypted with B's public key.

Integrity

- Is the main property provided by hash functions and message authentication codes;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;
- MACs provide integrity coupled with authentication;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;
- MACs provide integrity coupled with authentication;
- Integrity provided by theses cryptographic primitives are intended to detect active modification of messages;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;
- MACs provide integrity coupled with authentication;
- Integrity provided by theses cryptographic primitives are intended to detect active modification of messages;
- Integrity functions can also be used to avoid homomorphic manipulation;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;
- MACs provide integrity coupled with authentication;
- Integrity provided by theses cryptographic primitives are intended to detect active modification of messages;
- Integrity functions can also be used to avoid homomorphic manipulation;
- Can be used to avoid reverting operations within protocols;

Integrity

- Is the main property provided by hash functions and message authentication codes;
- Hash function provide “clean cut” integrity checking;
- MACs provide integrity coupled with authentication;
- Integrity provided by theses cryptographic primitives are intended to detect active modification of messages;
- Integrity functions can also be used to avoid homomorphic manipulation;
- Can be used to avoid reverting operations within protocols;
- On itself is a weak property.

Integrity Examples

- A sends to B the hash of message M;

Integrity Examples

- A sends to B the hash of message M;
- A sends to B the authentication code of message M with Key Kab.

Timeliness

- Anchor the messages to the correct timing;

Timeliness

- Anchor the messages to the correct timing;
- Can be provided by nonces (number used only once);

Timeliness

- Anchor the messages to the correct timing;
- Can be provided by nonces (number used only once);
- Can be provided by Timestamps;

Timeliness

- Anchor the messages to the correct timing;
- Can be provided by nonces (number used only once);
- Can be provided by Timestamps;
- Timestamps are usually coupled with time to live requirements;

Timeliness

- Anchor the messages to the correct timing;
- Can be provided by nonces (number used only once);
- Can be provided by Timestamps;
- Timestamps are usually coupled with time to live requirements;
- Allows for peers to check the ordering of messages;

Timeliness

- Anchor the messages to the correct timing;
- Can be provided by nonces (number used only once);
- Can be provided by Timestamps;
- Timestamps are usually coupled with time to live requirements;
- Allows for peers to check the ordering of messages;
- Allows for peers to check the liveness of other peers.

Timeliness Examples

- A sends to B the nounce Na and recieves back Nb,Na ;

Timeliness Examples

- A sends to B the nounce Na and recieves back Nb,Na ;
- A sends to B the timestamp of the generation time of the messages.

Authentication

- Is a basic but usually composed property;

Authentication

- Is a basic but usually composed property;
- Comes in different shapes depending on the basic building blocks used;

Authentication

- Is a basic but usually composed property;
- Comes in different shapes depending on the basic building blocks used;
- Aliveness - A runs the protocol with B;

Authentication

- Is a basic but usually composed property;
- Comes in different shapes depending on the basic building blocks used;
- Aliveness - A runs the protocol with B;
- Weak Agreement - A runs the protocol with B but B does not authenticate A;

Authentication

- Is a basic but usually composed property;
- Comes in different shapes depending on the basic building blocks used;
- Aliveness - A runs the protocol with B;
- Weak Agreement - A runs the protocol with B but B does not authenticate A;
- Non-Injective Agreement - Key exchange;

Authentication

- Is a basic but usually composed property;
- Comes in different shapes depending on the basic building blocks used;
- Aliveness - A runs the protocol with B;
- Weak Agreement - A runs the protocol with B but B does not authenticate A;
- Non-Injective Agreement - Key exchange;
- Mutual Agreement - A runs the protocol with B but B does authenticate A.

Two facets of authentication

- Authentication can serve both for assigning responsibility and for giving credit;

Two facets of authentication

- Authentication can serve both for assigning responsibility and for giving credit;
- An “authenticated” message M from a principal A to a principal B may be used in at least two distinct ways:

Two facets of authentication

- Authentication can serve both for assigning responsibility and for giving credit;
- An "authenticated" message M from a principal A to a principal B may be used in at least two distinct ways:
  - B may believe that the message M is being supported by A's authority;

Two facets of authentication

- Authentication can serve both for assigning responsibility and for giving credit;
- An "authenticated" message M from a principal A to a principal B may be used in at least two distinct ways:
  - B may believe that the message M is being supported by A's authority;
  - B may attribute credit for the message M to A.

Two facets of authentication

- Authentication can serve both for assigning responsibility and for giving credit;
- An "authenticated" message M from a principal A to a principal B may be used in at least two distinct ways:
  - B may believe that the message M is being supported by A's authority;
  - B may attribute credit for the message M to A.

Two facets of authentication

- Some protocols are adequate for assigning responsibility but not for giving credit, and vice versa;

Two facets of authentication

- Some protocols are adequate for assigning responsibility but not for giving credit, and vice versa;
- The two facets of authentication are most clearly separate in protocols that rely on asymmetric cryptosystems;

Two facets of authentication

- Some protocols are adequate for assigning responsibility but not for giving credit, and vice versa;
- The two facets of authentication are most clearly separate in protocols that rely on asymmetric cryptosystems;
- Even when it is proved beyond a reasonable doubt that a principal sent a message, responsibility and credit may not follow.

Views on responsibility and credit

- An authentication protocol should at least establish responsibility;

Views on responsibility and credit

- An authentication protocol should at least establish responsibility;
- There does not seem to be a consensus that an authentication protocol should also establish credit;

Views on responsibility and credit

- An authentication protocol should at least establish responsibility;
- There does not seem to be a consensus that an authentication protocol should also establish credit;
- Once a protocol has set up a channel that speaks for a principal, it is easy to use the channel for establishing credit whenever the need arises;

Views on responsibility and credit

- An authentication protocol should at least establish responsibility;
- There does not seem to be a consensus that an authentication protocol should also establish credit;
- Once a protocol has set up a channel that speaks for a principal, it is easy to use the channel for establishing credit whenever the need arises;
- Establishing credit is a matter of prudence.

Analysis of Authentication

- Honest protocol participants are expected to follow the rules of the protocol faithfully,and not to try to obtain credit for messages that they did not generate themselves. A proof about honest protocol participants may show that a protocol establishes responsibility, but not credit;

Analysis of Authentication

- Honest protocol participants are expected to follow the rules of the protocol faithfully,and not to try to obtain credit for messages that they did not generate themselves. A proof about honest protocol participants may show that a protocol establishes responsibility, but not credit;
- When an attacker is included as protocol participant, the attacker is not forced to follow the rules of the protocol, and may attempt to get undue credit. A proof that concerns such an attacker can show that a protocol establishes credit.

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?

Discussion

- Can give examples of security protocols that have these properties we shown above?

Discussion

- Can give examples of security protocols that have these properties we shown above?
- Can you give examples of problems/attacks on security protocols that have these properties we shown above?

Discussion

- Can give examples of security protocols that have these properties we shown above?
- Can you give examples of problems/attacks on security protocols that have these properties we shown above?
- How can we avoid problems/attacks on security protocols?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA