Security Properties

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

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.

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