INFORMATION SECURITY
lectures by Ferucio Laurentiu Tiplea

Introduction to Information Security

Prof.dr. Ferucio Laurențiu Țiplea

Fall 2023

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Security properties

Security threats and attacks

Reading and exercise guide

Security properties

Information security: more important than ever!

"By reverse-engineering the communications between a Tesla Model Y and its credit card key, they were able to properly execute a range-extending relay attack against the crossover. While this specific use case focuses on Tesla, it's a proof of concept – NFC handshakes can, and eventually will, be reverse-engineered."

Schneier on Security

Relay attack against Teslas

Sept 15, 2022

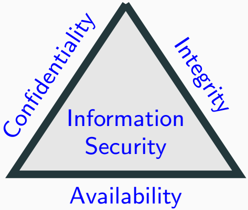
`https://www.schneier.com`

Modern trends raising security issues

- Distributed computing and remote access;
- Wireless devices;
- Electronic commerce, electronic payment;
- Electronic voting;
- Internet auctions, brokerage;
- Interactive games and lotteries;
- Cryptocurrencies and blockchain technologies.

Security properties

According to the NIST Computer Security Handbook from Guttman and Roback (1995) (see also Nieles et al. (2017)), information security rests on three security properties (the CIA triad):



Additional security properties are needed nowadays to capture current requirements better:

- Authentication;
- Accountability.

The interpretation of these security properties vary, depending on the context in which they arise.

Confidentiality, integrity, and availability

- Confidentiality – or secrecy, has a number of different meanings:
  - A very strict interpretation: the intruder should not be able to deduce anything about the legitimate users' activity (this is closely related to privacy);
  - In most cases: the intruder is not able to derive the plaintext of messages passing between honest users;
- Integrity – is usually taken to mean that data cannot be corrupted, or at least that any such corruption will always be detected;
- Availability – refers to the ability to use the information or resource (data or service) desired.

Authentication and accountability

- Authentication – this property embraces several forms such as:
  - Authentication of origin – taken to mean that we can be sure that a message that purports to be from a certain party was indeed originated by that party;
  - Entity authentication;
  - Key authentication;
- Accountability – there are many definitions for what it means to be accountable. One of them is:
  - Accountability should guarantee that the actions of an entity are traced uniquely to that entity.

Other security properties

- Non-repudiation – prevents either sender or receiver from denying a transmitted message;
- Fairness – occasionally, protocols are required to enforce certain fairness properties. In electronic contract signing, for example, we want to avoid one of the participants being able to gain some advantages over another by halting the protocol partway through;
- Anonymity – intuitively, a system that is anonymous over some set of events E should have the property that when an event from E occurs then an observer, though he may be able to deduce that an event from E has occurred, will be unable to identify which.

Security threats and attacks

Security threat, vulnerability, attack

- A security threat is a potential violation of security;
- A security violation need not occur for there to be a threat;
- A vulnerability is a flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy;
- Those actions that could cause a security violation to occur are called attacks;
- Those who execute attacks, or cause their execution, are called attackers or intruders.

Intruders

The objective of an intruder is to gain access to a system or to increase the range of privileges accessible on a system. Taxonomy of intruders:

- outsider: acts against the system from outside;
- insider: acts against the system from inside. Usually, an insider is more powerful than an outsider because he/she is a legitimate user who can have access to data, programs, or other resources;
- passive intruder: read messages and deduce information from them using public information;
- active intruder: can read messages, compose new messages, and send them in the system;
- coalition of individuals: an intruder is not necessarily just one individual. More individuals may share their common knowledge (public and secret) in order to get specific information.

Classes of security threats

A classification of security threats according to Shirey (2000) (see also Shirey (2007)) and based on threat consequences:

- disclosure – unauthorized access to information;
- deception – acceptance of false data;
- disruption – interruption or prevention of correct operation;
- usurpation – unauthorized control of some part of a system.

Examples of practical attacks

- Passive eavesdropping, sniffing, snooping
    - unauthorized interception of information;
    - it is a form of disclosure;
    - it is passive;
    - (passive) wiretapping is a form of snooping;
- Modification/alteration (sometimes called active eavesdropping, sniffing, or snooping)
    - unauthorized interception and change of information;
    - it may be a form of deception, disruption, or usurpation;
    - it is active;
    - active wiretapping is a form of modification;
- Masquerading/spoofing
    - impersonation of one entity by another;
    - it is a form of both deception and usurpation;
    - it may be passive or active;
    - delegation is not a violation of security;

Examples of practical attacks

- Repudiation of origin
  - a false denial that an entity sent or created something;
  - it is a form of deception;
- Denial of receipt
  - a false denial that an entity received some information or message;
  - it may be a form of deception;
- Delay
  - a temporary inhibition of a service;
  - it is a form of usurpation;
  - it may be passive or active;
- Denial of service
  - a long term inhibition of a service;
  - it is a form of usurpation;
  - it may be passive or active.

Social engineering attacks

In information security, social engineering is a form of psychological manipulation of people to determine them performing some actions or divulging confidential information.

Examples of attacks:

- Phishing;
- Vishing (voice phishing);
- Smishing (SMS phishing).

Attack strategies

Three well-known strategies an intruder might employ to attack the security of a system are in order:

- Man-in-the-middle;
- Interleave;
- Attacks that exploit design properties or software or hardware implementation properties.

Security analysis should not depend on knowing any attack strategy!

However, in practice, the security analysis is often done by considering the resistance to certain classes of attacks. Why? Because a general security analysis is practically infeasible in most cases.

Example of man-in-the-middle attack

This style of attack involves the intruder imposing himself between the communications between two parties. For instance, let us consider the following protocol based on a commutative cipher (K_u denotes user U's secret key).

Protocol 1 (Shamir's no-key protocol / Shamir's three-pass protocol)

$$\begin{array}{lll} 1. & A \rightarrow B: & \{x\}_{K_a} \\ 2. & B \rightarrow A: & \{\{x\}_{K_a}\}_{K_b} \\ 3. & A \rightarrow B: & \{x\}_{K_b} \end{array}$$

Goal: A sends x to B without knowing B's secret key.

Correctness of step 3: $\{\{x\}_{K_a}\}_{K_b} = \{\{x\}_{K_b}\}_{K_a}$ (by commutativity).

Man-in-the-middle cont'd

Attack 1 (Man-in-the-middle attack on Shamis's protocol)

- *C intercepts the first message, encrypts it*

$$\{\{x\}_{K_a}\}_{K_c},$$

  and returns it to A;
- *C intercepts $\{x\}_{K_c}$ from A and recovers x.*

Prevention of the attack – impossible over public Abelian groups: Onur et al. (2017).

For cryptographic protocols preventing the man-in-the-middle attack please see Katz (2002).

Example of interleave attack

This attack is based on impersonating legal users and interleave runs in the protocol. For instance, let us consider the Needham-Schroeder public-key protocol (N_u denotes U's nonce, and K_u is U's public key).

Protocol 2 (Needham-Schroeder public key protocol)

$$\begin{array}{lll} 1. & A \to B: & A, B, \{N_a, A\}_{K_b} \\ 2. & B \to A: & B, A, \{N_a, N_b\}_{K_a} \\ 3. & A \to B: & A, B, \{N_b\}_{K_b} \end{array}$$

Goal: A and B agree on the values of N_a and N_b, and no one else knows these values.

Lowe's attack

Attack 2 (Lowe (1995))

$$
\begin{array}{lll}
1. & A \to C: & A, C, \{N_a, A\}_{K_c} \\
2. & C(A) \to B: & A, B, \{N_a, A\}_{K_b} \\
3. & B \to C(A): & B, A, \{N_a, N_b\}_{K_a} \\
4. & C \to A: & C, A, \{N_a, N_b\}_{K_a} \\
5. & A \to C: & A, C, \{N_b\}_{K_c} \\
6. & C(A) \to B: & A, B, \{N_b\}_{K_b}
\end{array}
$$

where C is a recognized user, that is, he is known to the other users and has a certified public key. At the end of this:

- A thinks that he and C exclusively share knowledge of N_a and N_b;
- B thinks that he and A exclusively share knowledge of N_a and N_b.

Prevention of the attack – add identity of sender in step 2:

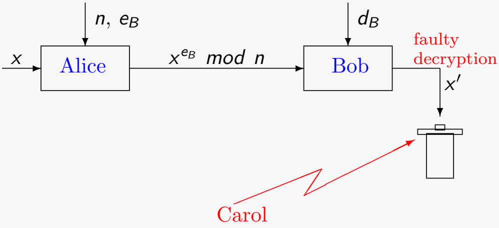
$$A, B, \{N_a, N_b, B\}_{K_a}$$

Example of attack exploiting faulty implementation

Faulty implementations of cryptographic protocols can provide valuable information to an intruder that can use them to break the system. The following example is due to a personal communication of Lenstra (see Boneh et al. (1997) and Boneh (1999)).

Protocol 3 (Encrypted communication by RSA)

public n ($n = pq$ – factoring intractable)
secret p, q (large prime numbers)



Lenstra's attack

Attack 3 (Lenstra's attack)

By the Chinese Remainder Theorem, x is the unique solution of the system

$$\begin{cases} x \equiv x_p \ mod \ p \\ x \equiv x_q \ mod \ q, \end{cases}$$

where $x_p = y^{d_B \ mod \ (p-1)} \ mod \ p$ and $x_q = y^{d_B \ mod \ (q-1)} \ mod \ q$.

Assume x_p was computed correctly, but not x_q, and let x' be the result obtained by the receiver by this erroneous decryption. x' is meaningless and, therefore, the receiver throw it away. If the intruder (C) is able to get x', then the intruder can recover p by the equation

$$p = (((x')^{e_B} - y) \ mod \ n, n).$$

In such a case, the cryptosystem is completely broken.

Formal analysis of security protocols

The difficulty of designing and analyzing security protocols stems from a number of considerations:

- The properties they are supposed to ensure are extremely subtle;
- These protocols inhabit a complex, hostile environment;
- Capturing the capabilities of intruders is inevitable extremely difficult;
- By their very nature security protocols involve a high degree of concurrency.

These facts lead to the undecidability of many security properties when studied on unrestricted protocols. On restricted protocols, they can become decidable, but even with severe restrictions, the complexity of their decision is very high. (see, for example Ţiplea et al. (2005), Ţiplea et al. (2008), Ţiplea et al. (2013)).

Reading and exercise guide

Reading and exercise guide

In addition to the bibliography already found on slides (that you can get by Google search on the net or by asking me), I recommend you:

1. Chapter 1 of Bishop (2005);
2. Chapter 1 of Stallings (2020).

References

Bishop, M. A. (2005). *Introduction to Computer Security*. Addison-Wesley.

Boneh, D. (1999). Twenty years of attacks on the rsa cryptosystem. *Notices of the AMS*, 46:203–213.

Boneh, D., DeMillo, R. A., and Lipton, R. J. (1997). On the importance of checking cryptographic protocols for faults. In Fumy, W., editor, *Advances in Cryptology — EUROCRYPT '97*, pages 37–51, Berlin, Heidelberg. Springer Berlin Heidelberg.

Ţiplea, F. L., Bîrjoveanu, C. V., Enea, C., and Boureanu, I. (2008). Secrecy for bounded security protocols with freshness check is NEXPTIME-complete. *J. Comput. Secur.*, 16(6):689–712.

Ţiplea, F. L., Enea, C., and Bîrjoveanu, C. V. (2005). Decidability and complexity results for security protocols. In *VISSAS*. IOS Press.

Ţiplea, F. L., Vamanu, L., and Vîrlan, C. (2013). Reasoning about minimal anonymity in security protocols. *Future Gener. Comput. Syst.*, 29(3):828–842.

Guttman, B. and Roback, E. (1995). An introduction to computer security: the NIST handbook. NIST Pubs 800-12, NIST.

Katz, J. (2002). *Efficient Cryptographic Protocols Preventing "Man-in-the-Middle" Attacks*. PhD thesis, Columbia University.

Lowe, G. (1995). An attack on the Needham-Schroeder public-key authentication protocol. *Inf. Process. Lett.*, 56(3):131–133.

Nieles, M., Dempsey, K., and Pillitteri, V. (2017). An introduction to information security. NIST Pubs 800-12 Rev. 1, NIST.

Onur, C. B., Kiliç, A., and Onur, E. (2017). Impossibility of three pass protocol using public Abelian groups. *CoRR*, abs/1703.06179.

Shirey, R. (2000). Internet security glossary. RFC 2828, GTE/BBE Technologies.

Shirey, R. (2007). Internet security glossary, vers. 2. RFC 4949, GTE/BBE Technologies.

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson, 8th edition.