Computer Security and Privacy (COM-301)

Week 1: Basic Concepts

Interactive Problem Solving

Establishing a security policy: When your adversary is the NSA…


swissinfo.ch
The Swiss voice in the world since 1935
GEOPOLITICS DEMOCRACY SCIENCE SWISS IDENTITY ECONOMY SWISS ABROAD
Swiss Politics

NSA accused of tapping Swisscom phone lines

swisscom

The Swiss Federal Prosecutor's Office is investigating whether America's National Security Agency (NSA) tapped Swisscom phone lines. The accusation comes from Austrian parliamentarian and whistleblower Peter Pilz.

May 27, 2015 - 17:42 1 minute

Establish what you are trying to protect:

- What is the **system** under attack?
- Who are the **principals**?
- What are their **assets**?
- What are the **security properties** to maintain?

Define against whom and how:

- What is the **threat model**?
- What would be your **security policy**?

https://www.swissinfo.ch/eng/politics/nsa-accused-of-tapping-swisscom-phone-lines/41454902

A high level analysis could be (very incomplete, sufficient for the purpose of the example):

The **system** under attack is the Swisscom communication infrastructure
The **principals** are Swisscom employees, and the Swisscom customer: people that use the infrastructure to make phone calls (the "callers").
-> More detail about the NSA as principal as discussed in INM202: The sentence "principals may not contain the adversary" in the slides is about the possibility that, once the principals are defined, the adversary can either be among the principals, or outside of the principals list. In this exercise, the NSA is not a principal as the NSA does not directly act on the assets of the system. There can be collusion, i.e., an NSA agent is a Swisscom customer (or employee), but even then, the principals only include customer (or employee), not NSA. The NSA agent should have the same rights as any Swisscom customer (or employee), not more. We are in the case where the list of principals does not contain the adversary.
The **assets** are, among others, the data sent through the communication infrastructure
The **security properties** to maintain are the confidentiality of communications, the integrity of communications, and the availability of communication

Threat model:

The NSA ! Big and powerful! State level adversary

Can observe Swisscom communication channels (e.g., an agent with an antenna)

Can hack Swisscom systems

Can corrupt Swisscom employees

Can corrupt phones of Swisscom users

A very high-level **security policy**:

- Only the callers can access the content of the communication (not Swisscom employees)
- No other than the caller can modify the content of the communication (not even Swisscom employees)
- No other that Swisscom employees can stop the system

Establishing a security policy: ...or a young hacker.

VAUD

Mots de passe et photos intimes dérobés à l'Unil

Un étudiant a piégé des ordinateurs publics, notamment à la bibliothèque de l'Unithèque, pour accéder aux comptes et télécharger des fichiers privés.

Un étudiant a obtenu des centaines de photos intimes en piratant des ordinateurs publics de l'Unil.

Establish what you are trying to protect:

- What is the **system** under attack?
- Who are the **principals**?
- What are their **assets**?
- What are the **security properties** to maintain?

Define against whom and how:

- What is the **threat model**?
- What would be your **security policy**?

https://www.20min.ch/ro/news/vaud/story/Mots-de-passes-et-photos-intimes-derobes-a-l-UNIL-23553124?httpredirect

Example Solution 1 – assuming that the attacker stole credential to access the IT system:

A high level analysis could be (very incomplete, sufficient for the purpose of the example)

The system under attack is the UNIL accounts
The principals are UNIL sysadmins, UNIL employees and students
The assets are, among others, the data stored in the students accounts
The security properties to maintain are the confidentiality of the accounts' content, the integrity of he accounts' content, and the availability of the accounts.

A very high-level security policy:
- Only the students can access the content of the their own accounts
- No other than the students can modify the content of the accounts
- No other that UNIL sysadmins can stop the system

Threat model:
Here we have one “weak” adversary with little resources.
- Cannot observe the full system
- Cannot corrupt other students
- Cannot corrupt the administrators
- Cannot hack UNIL backend
- Can corrupt a computer used by the students

Example Solution 2 – reading the article in more details, the computer were in "libre service", i.e. freely available with no authentication needed:

The system under attack can be: the openly available machines at UNIL
The principals are the users of these machines and the administrators of this machine
The assets are, among others, the keystrokes typed on these computers, and so in particular the identifiers and passwords of private accounts (gmail/facebook/instagram/…) of the users of these machines

The security properties to maintain are the confidentiality of the key typed by students on the keyboards of these machines’ content.

A very high-level security policy:
- Only the administrators and the students can get know the keystrokes that the student user typed
- No other student can know which key were typed by a previous/future user

Threat model:
- Cannot corrupt the administrators
- Can temper with/corrupt a freely available computer