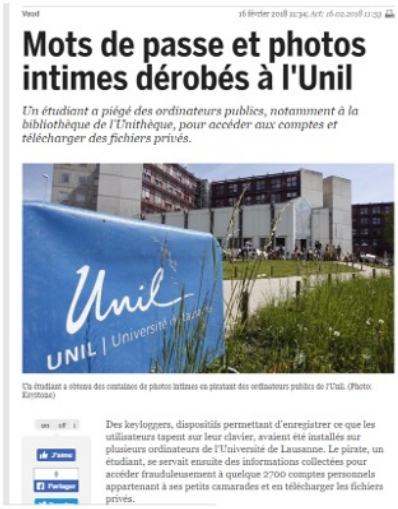
Establishing a security policy : Solo young hackers



Vaud

16 février 2018 11:34; Act: 16.02.2018 11:53

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. (Photo: Keystone)

Des keyloggers, dispositifs permettant d'enregistrer ce que les utilisateurs tapent sur leur clavier, avaient été installés sur plusieurs ordinateurs de l'Université de Lausanne. Le pirate, un étudiant, se servait ensuite des informations collectées pour accéder frauduleusement à quelque 2'700 comptes personnels appartenant à ses petits camarades et en télécharger les fichiers privés.

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

- 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

1

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:
This is very similar to the NSA case in the previous slides, but the threat model is very different. Here we have one "weak" adversary with little resources.
- Cannot observe the full system
- Cannot corrupt other students
- Cannot hack UNIL backend
- Can corrupt a computer used by the students

Establishing a security policy : State-level adversary

SUSPECTED SPYING

NSA accused of tapping Swisscom phone lines

By swissinfo.ch and agencies

IN DEPTH: NSA SPYING

MAY 27, 2015 - 17:02

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.

According to Pilz, Germany's foreign intelligence service gathered data from several countries on behalf of the NSA. Pilz presented a number of relevant documents in Bern on Wednesday, including a list of key transmission lines. A list from 2005 showed nine Swisscom lines ending in Switzerland: seven in Zurich, two in Geneva.

Swisscom phone lines have allegedly been tapped by the NSA

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

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

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

2

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

The app of your dreams

SATELLITE
bar · concerts · cafés-théâtres

Based on a recommendation from a friend, you have recently installed a new app on your phone that allows you to pre-order drinks at Satellite to avoid long queues on busy nights. The app is connected to your CAMIPRO account so that, once you have ordered the drinks through the app, your order is directly paid for from your account. Access to the app is PIN-restricted and each user can choose their own PIN when they first register.

Describe a **security threat** to this system, a **potential vulnerability** of the system in relation to this threat, and the **harm** that could result from a successful attack within this threat model. Propose an additional **security mechanism** that the developers should implement to minimise this threat.

Example of correct answers:

Security threat -> A friend could learn my password and get access to my phone, and therefore could access my app
Vulnerability -> Weak PIN, easy to eavesdrop when ordering a drink. Phone might be on the table and easy to steal
Harm -> The friend is able to order a drink using my money
Security mechanism -> For example: biometric check when ordering (faceID) or 2FA (show camipro when getting drink)