

# La sécurité

## HEG-ID — Infobase

Alexandre Boder   Igor Milhit   Raphael Rey

Haute École de Gestion de Genève  
Filière Information Documentaire

2014

**h e g**



Haute école de gestion  
Genève

# La sécurité ?

- Qu'est-ce que **la sécurité** vous évoque ?

Identification /  
Authentification

Définitions

Fonctions

Mot de passe

Sécurité des  
données

Sauvegardes

Chiffrement

Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

SSI

Définitions

Risques

# La sécurité ?

- Worlds biggest data breaches hacks

Identification /  
Authentification

Définitions

Fonctions

Mot de passe

Sécurité des  
données

Sauvegardes

Chiffrement

Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

SSI

Définitions

Risques

# La sécurité ?

- Worlds biggest data breaches hacks
- ~~Le site est mort, vive le site !~~ et ~~mavenhosting~~

# La sécurité ?

- Worlds biggest data breaches hacks
- ~~Le site est mort, vive le site !~~ et mavenhosting
- Journée portes ouvertes du groupe UMP au Sénat

## Identification / Authentification

Définitions

Fonctions

Mot de passe

## Sécurité des données

Sauvegardes

Chiffrement

## Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

## SSI

Définitions

Risques

# 1 Identification / Authentification

## Identification / Authentification

Définitions

Fonctions

Mot de passe

## Sécurité des données

Sauvegardes

Chiffrement

## Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

## SSI

Définitions

Risques

## 1 Identification / Authentification

## 2 Sécurité des données

Identification /  
Authentification

Définitions

Fonctions

Mot de passe

Sécurité des  
données

Sauvegardes

Chiffrement

Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

SSI

Définitions

Risques

## 1 Identification / Authentification

## 2 Sécurité des données

## 3 Menaces



## Identification / Authentification

Définitions

Fonctions

Mot de passe

## Sécurité des données

Sauvegardes

Chiffrement

## Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

## SSI

Définitions

Risques

# 1 Identification / Authentification

# 2 Sécurité des données

# 3 Menaces

# 4 SSI

# Structure

## 1 Identification / Authentification

Définitions

Fonctions

Mot de passe

## 2 Sécurité des données

## 3 Menaces

## 4 SSI

# Identification

## Définition

"[...] en informatique, l'**identification** permet de connaître l'identité d'une entité, souvent à l'aide d'un identifiant tel qu'un nom d'utilisateur." (Wikipédia)

# Identification

## Définition

"[...] en informatique, l'**identification** permet de connaître l'identité d'une entité, souvent à l'aide d'un identifiant tel qu'un nom d'utilisateur." (Wikipédia)

- Nom, prénom
- Pseudo, nickname
- Adresse e-mail
- Biométrie ?

# Authentification

## Définition

"L'**authentification** est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources [...]." (Wikipédia)

# Authentification

## Définition

"L'**authentification** est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources [...]." (Wikipédia)

- mot de passe
- passphrase
- carte d'identité, passeport

# Identification

Ordinateur personnel

- Administrateur
- Utilisateur 1
- Utilisateur 2
- Visiteur
- ...

# Identification

Ordinateur personnel

## Question

Que peut-on faire en accédant à votre ordinateur personnel, avec votre session ouverte ?



# Identification

Ordinateur personnel

## Question

Que peut-on faire en accédant à votre ordinateur personnel, avec votre session ouverte ?

- Accéder aux données
- Aux mots de passes du navigateur
- → Aux comptes en lignes
- e-mail
- Droits d'administration (installation...)

# Des idées ?

## Question

Qu'est-ce qu'un bon mot de passe ?

# Règles

création

- Pas de mot de dictionnaire ou de nom propre
- Pas de date, de numéro postal ou d'année
- 8 caractères au minimum
- alphabet, minuscule, majuscule, chiffre, caractères spéciaux
- passphrase
- aléatoire

# Règles

## gestion

- **NE JAMAIS DIVULGUER**
- Ne pas les écrire
- Ne pas le communiquer par e-mail
- Ne pas utiliser 2x le même mot de passe
- Changer régulièrement
- Gestionnaire de mot de passe : Keepass  
<http://keepass.info/>  
Lastpass <https://lastpass.com/>

# Protection

## Question

Est-ce que le mot de passe est suffisant ?

# Structure

1 Identification / Authentification

2 Sécurité des données  
Sauvegardes  
Chiffrement

3 Menaces

4 SSI

# Définitions

sauvegarde

## Définition

"En informatique, la **sauvegarde** (backup en anglais) est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique." (Wikipédia)

- $\neq$  enregistrement
- $\neq$  archivage
- $\neq$  synchronisation
- *Quid* du cloud ?

# Définitions

## Définitions

**Externe** : la sauvegarde doit être faite sur un support indépendant du système informatique concerné

**Distante** : la sauvegarde peut être réalisée sur un support situé dans un lieu indépendant, par exemple via le réseau



# Distante

difficultés

- Connexion sécurisée
- Données chiffrées

# Définitions

types de sauvegardes

## Définitions

**Complète** : "consiste à copier toutes les données à sauvegarder que celles-ci soient récentes, anciennes, modifiées ou non." (Wikipédia)

**Différentielle** : copie uniquement ce qui a changé depuis la dernière sauvegarde complète

**Incrémentale** : copie uniquement ce qui a changé depuis la dernière sauvegarde différentielle

# Définition

## restauration

## Définition

La **restauration** consiste à rétablir les données à partir des sauvegardes. La méthode et les possibilités dépendent notamment du type de sauvegarde utilisé.

# Définitions

## Définitions

**Crypter, cryptage, etc.** : n'existent pas en français

**Chiffrer** : "transcrire des messages en un langage secret." (TLFi)

**Déchiffrer** : transcrire en langage clair un message codé, en possédant la clé

**Décrypter** : décoder un message sans connaître la clé

# Définitions

## Définitions

**Algorithme** : suite de processus, ou d'étapes permettant de chiffrer/déchiffrer

**Clé de chiffrement** : un des paramètres de l'algorithme, sur lequel repose la sécurité du chiffrement

# Chiffres

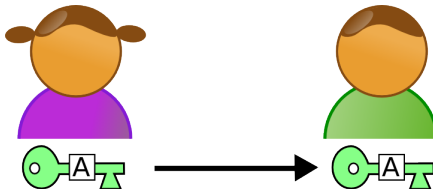
Table de Vigenère.

	Lettre en clair																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Chiffre de César
- Chiffre de Vigenère

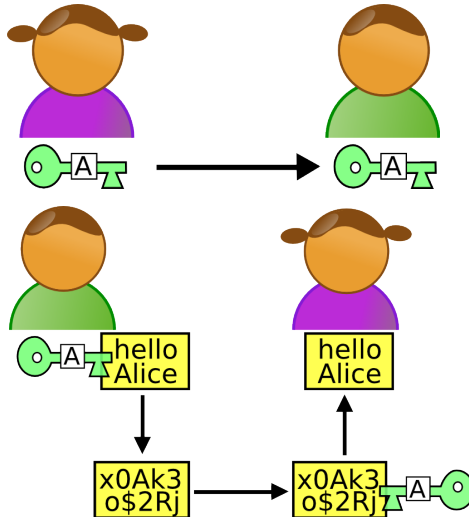
# Méthodes

Symétrie



# Méthodes

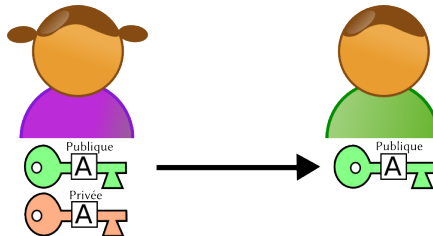
Symétrie





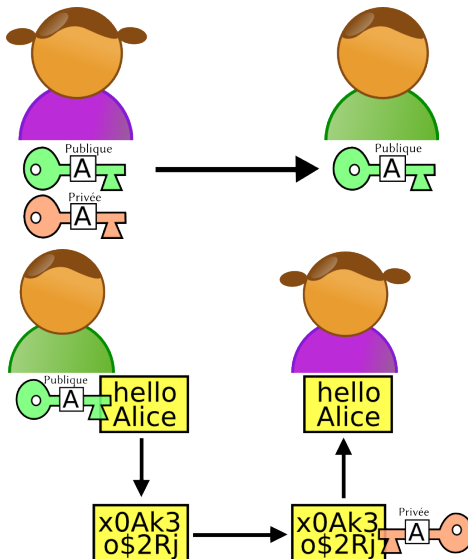
# Méthodes

## Asymétrie



# Méthodes

## Asymétrie



# Utilisations

- Communications chiffrées
  - e-mail
  - Instant Messaging
  - VoIP
- Connexions chiffrées
  - HTTPS
  - VPN
- Données chiffrées
  - Fichier
  - Répertoire
  - Partition (Disque)
  - Données stockées sur les serveurs d'autrui ("cloud")

# Fonction de hachage

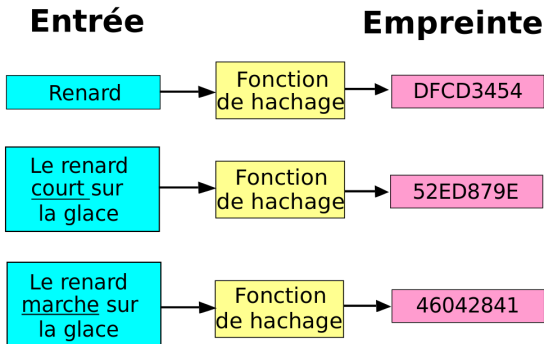
## Définition

"On nomme **fonction de hachage** une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien que incomplètement, la donnée initiale." (Wikipedia)

# Fonction de hachage

## Définition

"On nomme **fonction de hachage** une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien que incomplètement, la donnée initiale." (Wikipedia)



# Signature

## Définition

Technique informatique qui permet d'assurer l' **intégrité** et l' **authenticité** d'un document électronique, au moyen de la fonction de hashage et du chiffrement.

# Structure

1 Identification / Authentification

2 Sécurité des données

3 Menaces  
Logiciels Malveillants  
Autres menaces  
Objectifs  
Protection

4 SSI

# Adwares

## Définition

Un **Adware**, ou **publiciel** est un logiciel qui insère de la publicité à l'installation, par exemple sous la forme d'une barre d'outil ou de la configuration d'un moteur de recherche "exotique" par défaut.



# Virus

## Définitions

Un **virus** est un programme qui se réplique lui-même, avec pour but de se propager d'un ordinateur à l'autre au moyen d'un "hôte", le plus souvent un logiciel.

# Ver

## Définition

Contrairement au virus, le **ver** n'a pas besoin d'"hôte" pour se reproduire et se propager.

# Cheval de Troie

## Définition

Un **cheval de Troie** est un logiciel d'apparence légitime qui, en plus des fonctions attendues par l'utilisateur, exécute des fonctions sans que l'utilisateur s'en aperçoive. (Wikipedia)

# Spywares

## Définition

Un **logiciel espion** ou **mouchard** est comme son nom l'indique un logiciel qui a pour objectif d'intercepter l'activité d'un utilisateur, le plus souvent dans un contexte d'espionnage industriel.

# Keylogger

## Définition

Un **keylogger** (ou enregistreur de frappe) est un logiciel qui peut enregistrer l'activité du clavier et peut donc être utilisé pour intercepter les mots de passe ou dans un but d'espionnage industriel.

# Porte dérobée

## Définition

Une **porte dérobée**, ou **backdoor** est une fonctionnalité inconnue de l'utilisateur qui donne accès à un utilisateur externe au logiciel, voire au hardware.

# Hameçonnage

## Définition

Le **hameçonnage** ou le **phishing** consiste à diriger un internaute sur un site web leurre, afin de lui soutirer des informations confidentielles

# Ingénierie sociale

## Définition

L'**ingénierie sociale** est une technique d'attaque qui ne repose pas sur des moyens technologique mais sur les comportements humains.



Les **logiciels malveillants** ont pour objectifs :

- d'accéder aux données et/ou les détruire
- d'accéder au système informatique et/ou le détruire
- d'utiliser le système informatique pour :
  - diffuser des virus
  - envoyer des spams
  - attaquer d'autres systèmes informatique (ex : DDOS)

# Anti-virus

## Définition

Un **anti-virus** est un logiciel qui identifie, isole ou détruit un virus.

# Pare-feu

## Définition

Un **pare-feu** ou **firewall** est un système qui empêche les accès non autorisés depuis un réseau privé, ou à partir d'un réseau privé.

(<https://wiki.debian.org/Firewalls>)

# La sécurité

AB / IM / RR

## Identification / Authentification

Définitions

Fonctions

Mot de passe

## Sécurité des données

Sauvegardes

Chiffrement

## Menaces

Logiciels Malveillants

Autres menaces

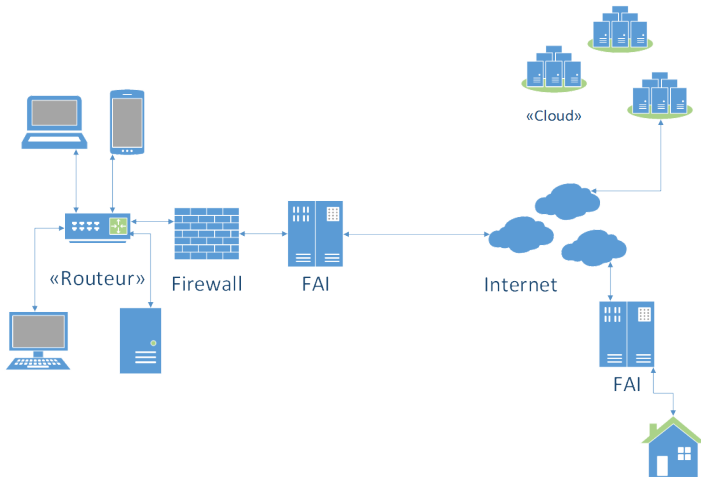
Objectifs

**Protection**

## SSI

Définitions

Risques



# Structure

1 Identification / Authentification

2 Sécurité des données

3 Menaces

4 SSI

Définitions

Risques

## Identification / Authentification

Définitions

Fonctions

Mot de passe

## Sécurité des données

Sauvegardes

Chiffrement

## Menaces

Logiciels Malveillants

Autres menaces

Objectifs

Protection

## SSI

Définitions

Risques

## Définition

La **sécurité des système d'information (SSI)** comprend l'ensemble des moyens pour garantir la protection d'un système d'information.

# Données

## Intégrité

- des données : les données ne doivent pas être détruites ou altérées de manière non autorisée.
- du système : le système doit faire ce qu'on lui demande sans modification non autorisée.

# Données

## Intégrité

- des données : les données ne doivent pas être détruites ou altérées de manière non autorisée.
- du système : le système doit faire ce qu'on lui demande sans modification non autorisée.

## Disponibilité

Les données doivent être accessibles en tout temps. Ou, du moins, de manière satisfaisante pour les besoins.



# Transactions

## Confidentialité

L'information ne doit être accessible et diffusée que par les personnes autorisées.

# Transactions

## Confidentialité

L'information ne doit être accessible et diffusée que par les personnes autorisées.

Contexte des bibliothèques ?

# Transactions

## Confidentialité

L'information ne doit être accessible et diffusée que par les personnes autorisées.

Contexte des bibliothèques ?

Adobe Digital Edition 4.0

# Transactions

## Authentification

Les acteurs doivent être identifiés et authentifiés, afin d'assurer la loyauté des transactions.

# Types de risques

- Protection de la vie privée
- Responsabilité civile et/ou pénale
- e-Réputation, confiance
- Pertes financières