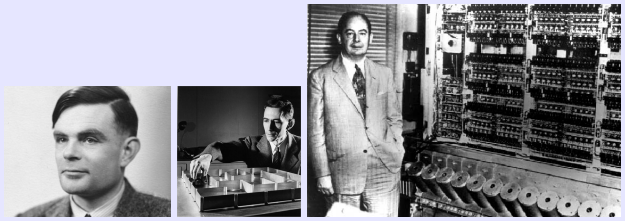


# Information, Calcul et Communication
## Module 3 : Systèmes

EPFL

# Information, Calcul et Communication
## Sécurité des systèmes informatiques (2/2)

Ph. Janson & J.-C. Chappelier

EPFL

## Motivations (rappel)

- L'univers numérique doit être sécurisé au même titre que le monde physique
- **La sécurité totale n'existe pas** plus dans le monde informatique que dans le monde physique
  - Un **compromis** entre le ***risque*** d'une attaque et le ***prix*** de la défense
- **Éduquer** les utilisateurs et les opérateurs est donc essentiel



## Menaces et défenses (rappel)

Les menaces sont :

- le *vol* d'informations
- la *manipulation* d'informations
- la *destruction* d'informations
- le *démenti*
- l'*usurpation d'identité*
- le *contournement* des défenses

Les combattre exige :

- **confidentialité** des informations
- vérification de l'**intégrité** des informations
- **disponibilité** des informations
- **responsabilisation** des utilisateurs
- **authentification** des utilisateurs/des processus
- hiérarchisation des **autorisations** des utilisateurs/des processus

☞ L'ultime objectif : contrôler qui a quel droit

# Cryptographie (rappel)

Il y a deux grandes familles de crypto-systèmes :

| | Symétrique à clés secrètes | Asymétrique à clés publiques |
|---|---|---|
| Exemples : | **One-time pad** | **RSA** |
| | DES | Diffie-Hellman |
| | AES | courbes elliptiques |
| Confidentialité : | oui | oui |
| Intégrité : | oui | oui |
| Responsabilité : | non | oui |

**Note :** on peut utiliser les deux en même temps (p.ex. envoi d'une clé privée symétrique par cryptage asymétrique)



# Objectifs de la leçon d'aujourd'hui

- Authentification
- Principales **règles de bonne conduite** des utilisateurs et administrateurs de systèmes informatiques
  pour se protéger contre les catastrophes (environnement), les hackers (humains) et leurs maliciels (technique) ?



# Authentification

**Menace :** usurpation d'identité

**Défense :** authentification :

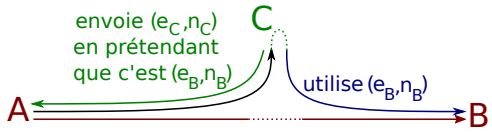
- par ce que l'on connaît
- par ce que l'on détient
- par ce que l'on est



# Exemple : authentification dans crypto-système asymétrique

Nous avons vu que dans un crypto-système asymétrique nous communiquons de façon confidentielle en utilisant la clé publique du destinataire.

Mais comment savoir que l'on envoie à la *bonne personne* et non pas à un fraudeur ?
(« *man-in-the-middle attack* »)




Comment savoir que l'on a la bonne clé publique ?

- Rencontrer physiquement la personne.
- Faire confiance à des tiers :
  ☞ **autorités de certification** qui distribuent les clés publiques

# Autorités de Certification des clés

Une autorité de certification (AC)

- délivre des certificats d'identités numériques
- offre les moyens de vérifier la validité des certificats qu'elle fournit

Certificat = message signé par une autorité de confiance

Plusieurs autorités de certification peuvent mutuellement certifier leurs clés publiques pour assurer l'authenticité des clés publiques de tiers certifiées par une autre AC

Exemples d'AC :

- locale : EPFL,
- globales : Symantec, Thawte, TBS



# Identité, sphère privée et réputation (1/2)

Nous avons tous une **identité** à plusieurs *facettes* :

- Citoyen
- Consommateur
- Employé ou indépendant
- Patient
- ...

Toutes ces facettes de notre identité ne sont pas (et n'ont pas à être) publiques.

- le vote d'un citoyen doit pouvoir rester secret ;
- l'opinion d'un consommateur doit pouvoir rester anonyme ;
- des collègues de travail peuvent avoir une liaison discrète tout à fait honorable ;
- quelqu'un doit pouvoir acheter un médicament sans être suspecté de maladie...



# Identité, sphère privée et réputation (2/2)

Nous avons tous une **identité** à plusieurs facettes.

La **protection de la sphère privée** :

- consiste à garder ces facettes *isolées* les unes des autres ;
- **NE** consiste **PAS** à cacher des activités illégales / immorales.

La plupart des gens ne se soucient de la protection de leur sphère privée dans le monde numérique...
...jusqu'au jour où ils l'auront perdue !

☞ L'enjeu est l'**intégrité de leur réputation**



# Limites de la protection de la sphère privée

- La **protection de la sphère privée** est un droit fondamental ;
- mais la société a besoin de **responsabilité** pour trouver et punir les activités illégales / immorales.

☞ **Où est la limite entre surveillance et espionnage ?**

Par exemple :

- Utiliser un GPS pour localiser un véhicule volé peut être légitime ;
- utiliser le même GPS pour faire suivre son chauffeur est abusif.
- Déposer une plainte anonyme contre un employeur frauduleux semble légitime ;
- colporter un ragot anonyme qui peut nuire à la répudation d'un tiers est abusif.

- *Pas de réponse absolue* et donc pas de réponse dans ce cours
- *Chaque société doit **pouvoir décider** pour elle-même* où sont les limites qu'elle accepte (des deux cotés)

## Menaces sur la sphère privée

Le fond de commerce des réseaux sociaux est notre sphère privée.

(« *In the world of Big Data, privacy invasion is the business model !* » (CNET 2012-02-29)
« *Si c'est gratuit, c'est que c'est vous le produit !* » (anonyme) )

De plus en plus de données privées sont :

- **récoltées** électroniquement
- **stockées** numériquement
  En des lieux et sous des juridictions que le « cloud » rend flous.
- **échangées** informatiquement
  Des entreprises commerciales vivent de la revente de ces données privées.
- **analysées** automatiquement
  Des entreprises sont spécialisées dans la *corrélation* de données isolées.
- **publiées** numériquement  No comment...
- **maintenues** par des tiers

☞ La sphère privée échappe de plus en plus aux intéressés eux-mêmes.
Obtenir assez de données privées pour usurper une identité devient de plus en plus facile.



## Sphère privée – Politique de protection

Au-delà de l'**accès** (*autorisation*), la protection de la sphère privée est aussi concernée par l'**usage** des informations.

Le contrôle de l'*usage* requiert une **politique** stipulant :

- **quelles** informations sont **collectées**
- **comment** les informations sont sécurisées
- combien de **temps** elles sont **gardées** (avant d'être effacées)
  Nous ignorons totalement les conséquences de vivre dans un monde qui n'oublie plus jamais rien !
- à quelles fins elles peuvent être **utilisées**
- à **qui** elles peuvent être **transmises**

Ces politiques doivent aussi garantir un **contrôle** aux individus concernés :
ils doivent avoir le droit de

- **inspecter** ce qui est collecté
- **corriger** ce qui est collecté
- être **informés** en cas de violation
- faire **appel** en cas de litige



## Authentification : moyens

Authentifier l'utilisateur par quelque chose qu'il

- connaît : **mots de passe**
- détient : **jetons**
- est : **biométrie**



## Authentification par connaissances : mots de passe

- Les mots de passe doivent être **stockés** sur l'ordinateur qui les vérifie
  ☞ Ils sont exposés ☞ Il **ne faut pas les stocker en texte clair**
- Les mots de passe doivent être **transmis** à l'ordinateur qui les vérifie
  ☞ Ils sont exposés ☞ Il **ne faut pas les transmettre en texte clair**
- Les mots de passe doivent être **saisis**
  ☞ Ne pas les exposer (« shoulder surfing »)
  - supprimer leur affichage à l'écran
  - cacher leur saisie
  - s'assurer qu'aucune caméra ne surveille
  - s'assurer qu'aucun maliciel n'espionne (key-logger – risque majeur) ou n'enregistre les émanations électromagnétiques

**Note :** pour protéger les identités, les *userids* devraient être aussi difficiles à deviner que les mots de passe.

# Le dilemme des mots de passe

mot de passe = identification par ce que **vous** (!) connaissez
(= et non **pas** quelqu'un d'autre)

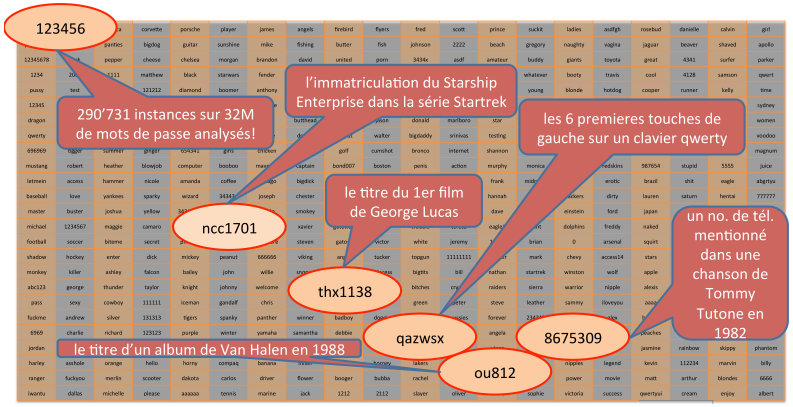
Les mots de passe ne doivent **JAMAIS** être écrits nulle part !

☞ Ils doivent être *facile à mémoriser* – mais *difficile à deviner* ! !

Comment faire ?



# Mots de passe les plus fréquents/stupides




Source : Perfect Passwords, Mark Burnett, 2005.

Voir aussi : https://en.wikipedia.org/wiki/List_of_the_most_common_passwords



# Mauvais mots de passe

- Environ 10% des gens utilisent au moins un mot de passe de la liste précédente
- Et 2% des gens utilisent un des 20 premiers mots de passe de cette liste
- Près de 50% des gens utilisent des noms, de l'argot ou des mots de passe triviaux (touches de clavier, lettres, ou chiffres consécutifs, etc.)

☞ Les utilisateurs sont si prévisibles que les pirates utilisent précisément ces trucs, pour tenter de pénétrer les ordinateurs en se faisant passer pour leurs victimes.
C'est ce qu'on appelle les **attaques au dictionnaire** de mots de passe.



# Comment choisir votre mot de passe

mot de passe = identification par ce que **vous** (!) connaissez

- Les mots de passe ne doivent **JAMAIS** être écrits nulle part (ni transmis à des tiers)
- Ils doivent être facile à mémoriser – mais difficile à deviner
- Un mot de passe différent pour chaque site / chaque application
- Changer de mot de passe régulièrement (rappel : équilibre menace / défense)
- Utiliser une longueur suffisante (au moins 8, sinon 12 caractères)
- Utiliser des alphabets assez vastes
  - Majuscules + minuscules + chiffres (soient 62 caractères)
  - Caractères spéciaux (mais pas toujours acceptés)
- **Testez** vos mots de passe avec des outils **de confiance** (en particulier jamais à distance !) qui travaillent en mode crypté p.ex. https://ophcrack.sourceforge.net/ (EPFL)

# Comment choisir votre mot de passe

Les mots de passe doivent avoir une longueur $M$ suffisante pour résister aux devinettes.
Risque $R$ = durée de vie $D$ × fréquence des attaques $F$ / $T^M$ ($T$ : taille de l'alphabet)
d'où : $M > \log(D \times F/R)/\log(T)$
p.ex. : $8 > \log(100 \text{ jours} \times (100 \text{ par jour})/10^{-9})/\log(62)$

- Utiliser un alphabet assez vaste (augmenter $T$)
- Limiter la fréquence des attaques (diminuer $F$)
  (p.ex. terminer toute connection après quelques échecs)
- Changer de mot de passe régulièrement (diminuer $D$)
  et ne jamais réutiliser le même mot de passe sur plusieurs systèmes ("*password sloth*")
- Ne jamais choisir un mot de passe dans un langage naturel ou un dialecte quelconque
  - Remplacer des lettres par des chiffres évidents ne sert à rien
    (p.ex. 0 for O, 1 for I, 2 for Z, 3 for E, 4 for A, 5 for S, 6 for G, 7 for T, 8 for B, 9 for q)
  - Ne pas épeler à l'envers, éliminer les voyelles, employer lettres pour phonèmes, etc.
  - Si cela vous paraît malin, les auteurs d'attaques au dictionnaire y ont aussi déjà pensé !



# Comment choisir votre mot de passe

☞ avoir un schéma de génération
Exemple de schéma :

- une base fixe, de séquences de lettres peu probables
- base variable 1 : site application système
- base variable 2 : date/année (encodé à votre façon)
- nombre de lignes = durée de validité de la table
  (= nombre de mots de passe disponibles)
- nombre de colonnes = longueur des mots de passe.

| phrase fixe (p.ex. dans une langue étrangère) | | | | descripteur du système | | descripteur de l'année | |
|---|---|---|---|---|---|---|---|
| w | t | i | h | T | A | 2 | m |
| a | o | w | i | H | D | m | m |
| s | s | a | d | I | W | i | x |
| a | u | o | e | N | 5 | l | i |
| b | s | i | s | K | 1 | 1 | i |
| i | h | s | u | P | 0 | 3 | i |



# Autres « mots » de passe

- Phrases de passe : but : entropie plus grande (longueur $M$ plus grande),
  mais attention à la prédicabilité de la phrase ! ! (modèle de langue)
- Questions de passe : répondre à des questions personnelles subtilement choisies
  (les réponses ne doivent être connues que de vous *seul(e)* !)
- Graphes de passe : cliquer en séquence sur des images positionnées aléatoirement
- Algorithmes de passe :
  construire les mots de passe selon un algorithme simple mais secret
  (généralisation du « schéma de génération » précédent)



# Authentification à double canaux ou à double facteur

Quand les mots de passe ne sont plus assez sûrs pour une application critique, on peut avoir recours à

- une **authentification à double canal**

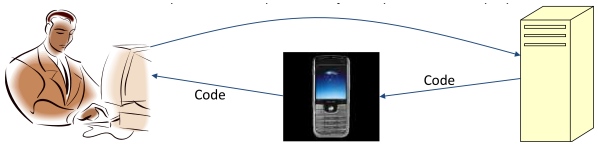

- L'ordinateur envoie un code aléatoire à l'utilisateur par un canal secondaire
  (p.ex. SMS comme le font par example Google, Swisscom, Telegram, etc.)
- L'utilisateur rentre le code dans son ordinateur
- Alternativement le téléphone mobile peut renvoyer un portrait de son propriètaire

NB : des hackers ont déjà surmonté une telle authentification

# Authentification à double canaux ou à double facteur

Quand les mots de passe ne sont plus assez sûrs pour une application critique, on peut avoir recours à

- une **authentification à double canal**

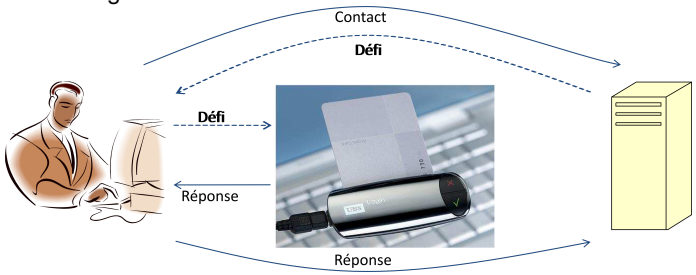



- ou une **authentification à double facteur** (ou même plus)
  - ☞ Biométrie ou jeton d'identification en plus du mot de passe



# Jeton : authentification par ce que l'on possède

- Basé sur un échange de codes ou un envoi de cachet-dateur chiffrés




- Avec un tel jeton non seulement l'utilisateur mais chaque transaction peut être identifiée
- Un maliciel ne peut pas interférer car l'utilisateur confirme chaque transaction sur le jeton



# Biométrie : authentification par ce que l'on est

- La biométrie est en fait la méthode d'authentification originelle de l'humanité ; ce qui est neuf est son utilisation en informatique.
- La biométrie d'un individu est unique mais pas secrète.
  - ☞ Le vol d'identité biométrique est donc un risque majeur ! (p.ex. copie d'empruntes digitales https://research.msu.edu/msus-3-d-hand-tests-fingerprint-scanners/ )
- La vérification biométrique est encline à erreurs :
  Des faux négatifs sont ennuyeux.
  Des faux positifs sont indésirables. (c'est le but de départ !)
  Trouver un compromis entre les deux est délicat...
  - ☞ La biométrie est souvent utilisée comme second facteur plutôt que comme seul facteur



# Techniques biométriques

- Profil et vitesse de dactylographie
  Peu précis
- Reconnaissance dynamique de signature
  Sûr mais cher
- Reconnaissance des veines de la paume de main (ou de la forme de la main)
  Sûr mais cher et peu pratique
- Reconnaissance des empreintes digitales
  Commune mais peu sûre
- Reconnaissance de la voix
  Ni très sûr ni très consistant (faux négatif)
- Reconnaissance du visage
  Ni très sûr (photo) ni très consistant (vieillissement)
- Reconnaissance de l'iris de l'oeil
  Pas très sûr à moins d'exiger un oeil « vivant »
- Reconnaissance de l'ADN
  Parfait ?... ...pour la science fiction ?

# Authentification bi-directionnelle

Toutes les techniques vues jusqu'ici n'offrent qu'une authentification *unidirectionnelle*, ce qui représente une carence et un risque majeur (« phishing ») :

Un service frauduleux peut se présenter sous l'identité d'un service réputé et ainsi récolter les identités et mots de passe d'utilisateurs innocents et crédules

Le premier partenaire qui s'identifie à l'autre doit lui révéler son identité (et son mot de passe ?)

**Solution :** identification **bi-directionnelle**

- Cryptographique de la part du service demandé (sur base de défi ou de cachet-dateur crypté)
- Cryptographique ou non de la part de l'utilisateur

C'est exactement ainsi que fonctionnent les protocoles HTTPS/SSL/TLS (indiqués par l'icône de cadenas dans la barre du navigateur) au moyen de certificats (AC)



# Conseils de « bonne conduite » (1/3)

**Authentification**

- Avoir de **vrais mots de passe sécurisés**, *différents* pour chaque poste/application
  ☞ schéma de génération de mots de passe
- **NE JAMAIS révéler** un mot de passe, à qui que ce soit !

**Données**

- Faire des copies de **sauvegardes** régulières
- **Crypter** ses données (p.ex. ses disques)
- Vraiment **écraser** (`shred`) toutes les données (ou détruire physiquement) sur tout support revendu/mis à la décharge
- Eviter l'usage de services publics (p.ex. Google Docs/Drive, calendar, contacts, iCloud, etc.) pour des informations confidentielles



# Conseil de « bonne conduite » (2/3)

**Protection de la machine**

- Installer anti-virus et pare-feu
- Toujours mettre à jour ses logiciels
- Ne jamais accepter un patch de logiciel quand on est connecté à un Wi-Fi public
- Condamner le partage de fichiers (et d'imprimantes)
- Condamner l'assistance à distance
- Ne jamais laisser un poste, ordi, téléphone ouvert : verrouiller l'écran, forcer la déconnexion automatique en cas de longue inactivité (15 min)
- se déconnecter systématiquement de toute machine/tout service en fin d'utilisation
- Ne jamais exécuter d'application en mode administrateur



# Conseil de « bonne conduite » (3/3)

**Protection de la machine** (suite)

- Interdire l'envoi automatique de notices d'absence – c'est une invitation au spam
- Se méfier des postes de travail et services publics – surtout gratuits

**Général**

- Se méfier de pirates en des lieux publics/hôtels – surtout dans les pays réputés « à risque »

**Navigation Internet**

- Ne pas accepter de script dans son navigateur
- Installer les plug-ins de sécurité de son navigateur (mais être sûr de leur qualité/intégrité ! !)
- Refuser systématiquement/Limiter le nombre de cookies

## Sécuriser votre wifi à la maison

1. Changer le mot de passe administrateur de votre routeur (souvent `192.168.1.1`)
   (trop souvent c'est le mot de passe « usine » qui est dessus, genre « `123456` », « `0123456` », « `12345678` », « `01234567` », « `000000` », « `00000000` », « `admin` », « `administrator` », etc.)
2. Ne faites pas vos opérations critiques (p.ex. banque) sur un wifi, mais sur un réseau Ethernet (cable)
3. Ayez au moins 2 réseaux wifi séparés :
   l'un pour vos accès perso privés critiques
   et un autres pour vos invités/amis/activités ludiques
4. Empêchez les matériels non autorisés à se connecter
   (filtrage d'adresses MAC)



## Résumé

- Catastrophes (environnement), hackers (humains) et maliciels (technique) représentent des menaces :
  - vol d'information
  - manipulation d'information
  - destruction d'information
  - démenti
  - usurpation d'identité
  - contournement des défenses
- qui visent nos données,
  - y compris celle de notre sphère privée ;
  - y compris notre identité et notre/nos réputation(s).



## Résumé

- Catastrophes (environnement), hackers (humains) et maliciels (technique) représentent des menaces
- qui visent nos données.
- Ces données doivent donc être
  - cryptées
  - sauvegardées
- et leur accès
  - authentifié (par ce que l'on connait, possède, est)
  - autorisé
- pour se défendre de façon appropriée (équilibre) et assurer :
  - confidentialité
  - intégrité
  - disponibilité
  - responsabilité
  - authentification
  - autorisation



## Résumé

L'éducation des utilisateurs et des opérateurs passe par l'enseignement de meilleures pratiques pour

- la prévention
- la surveillance
- la détection
- la correction

des menaces.

☞ Voir si nécessaire « *Pour aller plus loin* » en annexe

# Conclusion

- Sachez identifier les menaces et connaîssez les niveaux de défense appropriés
  (la sécurité totale n'existe pas !)
- Sauvegardez, cryptez vos données
- Choisissez bien, changez et protégez vos mots de passe
- D'une façon générale, adoptez de meilleures pratiques en vue d'une plus grande sécurité

Ceci termine ce cours I.C.C. !
En espérant que ce « voyage » annoncé dans la toute première leçon vous aura

- plu, intéressé, instruit.



# Annexe : Pour aller plus loin

- Le petit guide illustré EPFL « *Sécurité IT – Comment se prémunir contre les cyber-attaques* »
  https://www.epfl.ch/campus/services/wp-content/uploads/2018/11/Guide-securite-IT-Fr-web-vf.pdf
- Site EPFL « Sécurité IT »
  https://www.epfl.ch/campus/services/ressources-informatiques/secure-it/

- « *Guide des bonnes pratiques de l'Informatique* » de l'ANSSI française
  https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
- « Tout sur la sécurité informatique » de J.-F. Pillou et J.-Ph. Bay, Dunod, 5e édition, 2020.
  https://www.dunod.com/sciences-techniques/tout-sur-securite-informatique-0
- Et pour ceux qui voudraient aller encore plus loin, l'ANSSI française offre une pléthore de documents spécialisés gratuits :
  https://www.ssi.gouv.fr/administration/bonnes-pratiques/