Chapitre 1
Introduction à la sécurité et à la cryptologie

3éme licence informatique

Université de Jijel

janvier 2020

Plan

- Introduction à la sécurité et à la cryptologie
  - Définitions et exemples
  - Sécurité
  - Quels sont les risques liées à l'utilisation de l'informatique?
  - Apports de la cryptographie à la sécurité

Plan

1. Introduction à la sécurité et à la cryptologie
   - Définitions et exemples
   - Sécurité
   - Quels sont les risques liées à l'utilisation de l'informatique?
   - Apports de la cryptographie à la sécurité
2.
3.
4.

Sécurité informatique

- Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité de l'information, du système d'information et des systèmes et ressources informatiques.
- Notamment, on veut préserver
  - l'intégrité de l'information
  - La confidentialité de l'information
  - la disponiblité des systèmes
- Systèmes informatiques soumis à des menaces
  - utilisateur du système
  - personne malveillante
  - programme malveillant
  - sinistre (vol, incendie, dégât des eaux)

Cryptographie et cryptanalyse

[Source Wikipedia]

Definition (Cryptographie)

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

Definition (Cryptanalyse)

La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière.

Cryptographie : outil pour la sécurité informatique

Plan

Critères de sécurité

Mise en place de solutions de sécurité pour satisfaire

disponibilité : probabilité de bon fonctionnement, accessibilité, continuité de service

intégrité : certification de la non-altération des données, traitements et services

confidentialité : protection des données contre une divulgation non autorisée

authentification : vérification de l'identité de l'utilisateur et de ses autorisations

non-répudiation : imputabilité, traçabilité, auditabilité

Domaines d'intervention

sécurité physique

- environnement humain (politique de sécurité, éducation, charte)
- environnement matériel (incendie, dégâts des eaux, protection des salles, sauvegardes, alimentations électriques)

sécurité de l'exploitation

- hôte (système d'exploitation à jour, authentification) sécurité logique

données (accès aux fichiers, autorisations, chiffrements, sauvegarde)

- sécurité applicative

applications (virus, chevaux de troie, espiogiciels, spam, restrictions et
- localisations des applications)

sécurité des télécommunications

réseau interne (protocoles sécurisés)

- alentours (pare-feu, vpn)
-

Menaces informatiques

menace : action susceptible de nuire

vulnérabilité ou faille : niveau d'exposition face à une menace dans un certain contexte

contre-mesure ou parade : ensemble des actions mises en oeuvres en prévention d'une menace

attaque : exploitation d'une faille (d'un syst info) à des fins non connus de l'exploitant du système et généralement nuisibles

en permanence sur Internet par machines infectées rarement pirates

$$\text{Risque} = \frac{\text{Menace x Vulnérabilité}}{\text{Contre-mesure}}$$

Evaluation des risques liées à l'utilisation de l'informatique, Il importe de mesurer ces risques :

- en fonction de la probabilité ou de la fréquence de leurs survenances
- en mesurant leurs effets possibles.

Motivations des attaques

- intrusion dans le système
- vol d'informations industrielles (brevets), personnelles (bancaires), commerciales (contrats), organisationnelles
- troubler le bon fonctionnement d'un service (déni de service, *defacing*)
- utiliser le système comme rebond pour une autre attaque
- utiliser les ressources d'un système (ex : bonne bande passante)

Plan

1. Introduction à la sécurité et à la cryptologie
   - Définitions et exemples
   - Sécurité
   - Quels sont les risques liées à l'utilisation de l'informatique?
   - Apports de la cryptographie à la sécurité

Quels sont les risques liées à l'utilisation de l'informatique?

Ces effets peuvent avoir des conséquences **négligeables** ou **catastrophiques** :

— le traitement informatique en cours échoue : il suffit de le relancer, éventuellement par une autre méthode si on craint que la cause ne réapparaisse

— l'incident est bloquant et on doit procéder à une réparation ou une correction avant de poursuivre le travail entrepris.

Mais ces mêmes incidents peuvent avoir des conséquences beaucoup plus fâcheuses :

- données définitivement perdues ou altérées, ce qui les rend inexploitables ;
- données ou traitements durablement indisponibles, pouvant entraîner l'arrêt d'une production ou d'un service ;
- divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise ;
- déclenchement d'actions pouvant provoquer des accidents physiques ou induire des drames humains.

1. Les risques humains

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- a maladresse : commettre des erreurs : exécuter un traitement non souhaité, effacer involontairement des données ou des programmes, etc.
- l'inconscience et l'ignorance : introduire des programmes malveillants sans le savoir (par exemple lors de la réception de courrier).

De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent.
Réaliser des manipulations inconsidérées (autant avec des logiciels qu'avec du matériel)

1. Les risques humains

- la malveillance : impossible d'ignorer les différents problèmes de virus et de vers ces dernières années (beaucoup de couverture médiatique).

Certains utilisateurs peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données.

Il est facile pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent.

On parle alors de la « cyber-criminalité ».

1. Les risques humains

- l'ingénierie sociale (social engineering) est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins (publicitaires par exemple). Elle consiste à :

- se faire passer pour quelqu'un que l'on est pas (en général un administrateur)
- demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en inventant un quelconque prétexte (problème dans le réseau, modification de celui-ci, heure tardive, etc.).
- Elle peut se faire soit au moyen d'une simple communication téléphonique, soit par mail, soit en se déplaçant directement sur place.
- l'espionnage : surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc.

2. Les risques matériels

Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels. Ces incidents sont plus ou moins fréquents selon le soin apporté lors de la fabrication et l'application de procédures de tests effectuées avant que les ordinateurs et les programmes ne soient mis en service. Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc difficiles à prévoir.

- Incidents liés au matériel : la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts.
  Ils finissent un jour ou l'autre par tomber en panne.
  Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares.
  Parfois, elles relèvent d'une erreur de conception (une des toutes premières générations du
  processeur Pentium d'Intel pouvait produire, dans certaines circonstances, des erreurs de calcul) ;

2. Les risques matériels

- Incidents liés au logiciel : mais plus fréquents ;

les programmeurs peuvent faire des erreurs de manière individuellement ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.

- Incidents liés à l'environnement :

les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.

Il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles (et parfois celle des ordinateurs eux-mêmes !).

3. Crime informatique, cybercrime

- Crime informatique : délit où le système informatique est l'objet du délit et/ou le moyen de le réaliser.
- Cybercrime : forme du crime informatique qui utilise Internet
- en 2007, la cybercriminalité pèse 7,1 milliards de dollars aux USA
- en 2009, assignement en justice pour 559 millions de dollars aux USA (×2 en deux ans)
- Typologie : malveillance, erreur, accident Cibles : états, organisations,
- individus
- Vol d'identité, Chantage, Fraude financière, détournements de fonds, vol de biens virtuels, espionnage, cyberterrorisme, désinformation, apologies de crimes, escroqueries, atteinte aux mineurs, atteinte à la vie privée, incitation à la haine raciale, . . .

3. Crime informatique
→ Internet : un facteur aggravant

- dématérialisation des acteurs du délit, des objets du délit
- vulnérabilité : complexité des infrastructures informatique et réseaux
- automatisation, réalisation à grande échelle ⇒ partout, anonymat
- immatérialité : information numérique peut être détruite, modifiée, volé
- disponibilité d'outils, paradis numériques

  dépendance des états/organisations à l'informatique ⇒ facteur de risque ⇒ cyberterrorisme

3. Crime informatique
→Typologie des attaques

- accès physique : coupure électricité, vol de disque dur, écoute traffic réseau, récupération de matériels
- interception de communications : vol de session, vol d'identité, détournement de messages
- polupostage ou spam (98 % des mails)
- dénis de services : faiblesse de protocoles TCP/IP, vulnérabilité de logiciels serveurs
- intrusions : maliciels (virus, vers, chevaux de Troie), balayage de ports, élévation de privilèges
- trappes : porte invisiblee dans un logiciel ingénierie sociale : contact
- direct de l'utilisateur
- attention aux attaques par rebond : l'utilisateur "espion" peut voir sa responsabilité engagée.

3. Crime informatique

→Logiciels malveillants : Virus, Vers, troyens I

Virus Tout programme capable d'infecter un autre programme en le modifiant de façon à ce qu'il puisse se reproduire

Brain (premier sur PC en 1986), Netsky (2004, lit fichiers EML, HTML pour se propager par email), Sobig-F (2003, contient un serveur SMTP)

Infecte : Programmes, documents, secteurs de boot

Ver (Worm) Programme se propageant à travers le réseau

Blaster (Août 2003, faiblesse RPC Windows), Welchia (qqs jours après, élimine Blaster)

Troyen ou Cheval de Troie Programme à l'apparence utile mais cachant du code pour créer une faille dans le système (*backdoor*) BackOrifice, GrayBird (soi-disant nettoyeur de Blaster)

Porte dérobée (ou *backdoor*) Fonctionnalité inconnue de l'utilisateur, qui donne un accès secret au logiciel/système

Trusting Trust (1984), noyau Linux (2003)

3. Crime informatique

→Logiciels malveillants : Virus, Vers, troyens II

Machine zombie ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique (suite à une infection par ver/cheval de troie). Sert de rebond.

Botnet Réseau de machines zombies. Utile pour lancer des attaques, de déni de service ou spams

Bombes logiques Programme se déclencheant suite à un événement particulier (date, signal distant)

CIH/Chernobyl (déclenchement 26 avril 1999, 26 avril 1986)

Virus mutants réécriture de virus existants

Virus polymorphes modifie son apparence, pour ne pas être reconnu

Rétro-Virus attaque les signatures des antivirus

Virus boot Virus s'installant sur un secteur d'amorçage (clé usb , disque)

3. Crime informatique

→Logiciels malveillants : Virus, Vers, troyens III

- Virus d'applications (ou de document/macros) Programme infectant un document contenant des macros, exécutable par une application : VBScript
  - Concept (1995), Bubbleboy (1999, affichage du mail)
- Antivirus Logiciel de détection et suppression de virus et vers

- Méthodes : dictionnaires, heuristiques, comportements suspects, émulation (bac-à-sable)
- scanneurs sur accès : examine les fichiers/programmes à chaque accès
- scanneurs à la demande : examine les disques/fichiers/programmes suite à une demande

3. Crime informatique
→ Spywares : espiogiciels I

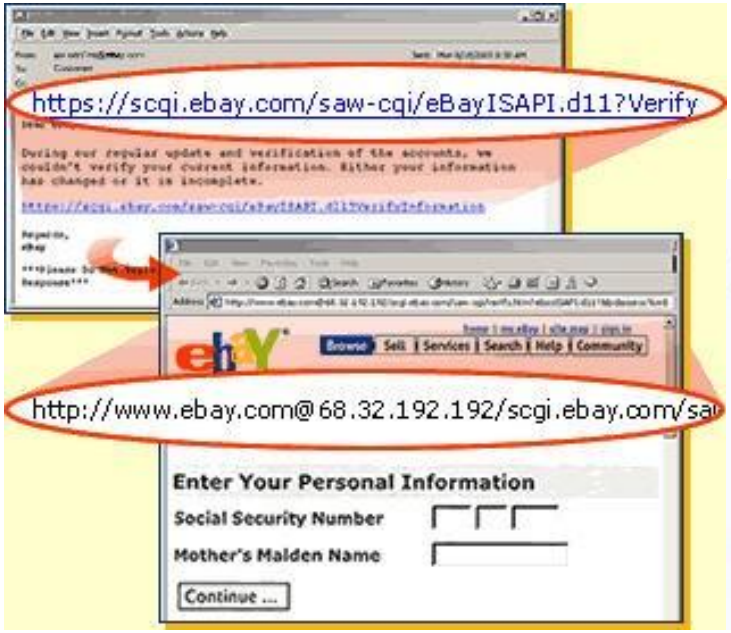
Espiogiciel Programme collectant des données sur un utilisateur, les envoyant à une société en général pour du profilage
- souvent avec des freewares ou sharewares
- Intégrés (PKZip, KaZaA, Real Player) ou externes
- souvent légaux (dans la licence)
- parades : ne pas installer de logiciels (!), antisypwares, firewall

keylogger enregistreur de touches : enregistrement des touches à l'insu de l'utilisateur. dispositif d'espionnage. Souvent un logiciel.

3. Crime informatique

→Menaces nouvelles I

Phishing/hameçonnage Arnaques via internet, usurper une identité fiable (genre banque), redirection vers site pirate ⇒ données bancaires, mots de passe



3. Crime informatique

→Menaces nouvelles II

Pharming (empoisonnement DNS) exploite une vulnérabilité pour rediger le trafic Internet d'un site Web vers un autre. Complémentaire de chevaux de Troie, spywares et phishing. Exemple : americanexpress.com, fedex.com, msn.com, Trendmicro.com (vulnérabilités dans le serveur DNS de Windows NT4 et Windows 2000, depuis corrigées).

Slamming fausse facture de renouvellement de nom de domaine et contrainte pour l'achat de noms de domaines proches, faux annuaires professionnels

3. Crime informatique

→Menaces nouvelles III

Vishing (VoIP + phishing). Serveurs VoIP appelant des numéros fixes, redirection vers boîte vocale informant d'anomalie, invitation à contacter un serveur vocal où il donnera ses coordonnées bancaires.

Ransomwares code malveillant (virus ou cheval de troie) cryptant certaines données, exige une rançon après pour le déchiffrement.

Exemple : Gpcode, scanne .xls .doc .txt .rtf ...

Cross Site Scripting (XSS) vulnérabilités dans serveur/app WEB pour insérer du code dans une page html renvoyée dynamiquement
Redirection vers un autre site, vol d'identifiant de session

Injection de code vulnérabilités dans serveurs/apps (SQL, WEB/XSS, LDAP

```
SELECT * FROM utilisateurs WHERE nom="\$nom";
// Saisie de : toto" OR 1=1 OR  nom="titi
SELECT * FROM utilisateurs WHERE nom="toto" OR  1=1 OR nom="titi";
```

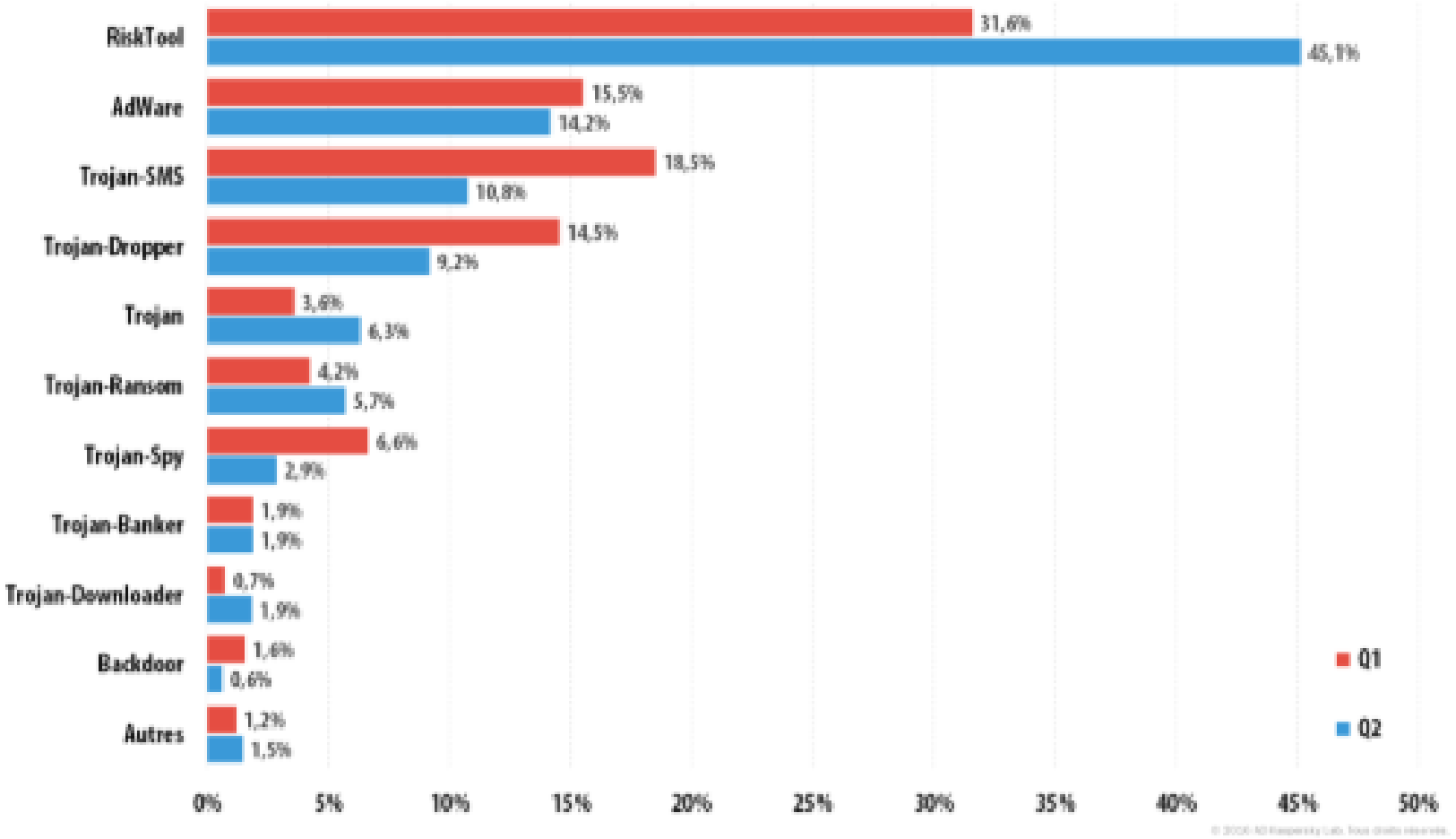
Chiffres et évolutions des menaces I

Kaspersky Lab, a annoncé Novembre 2017 les résultats d'une étude inédite sur les comportements et attitudes des professionnels par rapport à la sécurité informatique en Algérie

source: http://www.nticweb.com/webs/9173-etude-sur-la-s%C3%A9curit%C3%A9-informatique-en-alg%C3%A9rie.html

- 19% des professionnels interrogés n'utilisent pas de protection informatique, illustrant un niveau relativement élevé de vulnérabilité informatique des entreprises et organisations algériennes.
- 40% des répondants déclarent que leur entreprise a déjà été affectée par des menaces informatiques. Les virus , les logiciels malveillants (58%) et les logiciels espions (29%), forment le top des menaces les plus fréquentes.
- 68% des professionnels sondés ont déjà branché des clés USB inconnues sur leurs PC, là où 19% cliquent sur des pièces jointes qu'ils n'attendaient pas, incluses dans des mails envoyés par des inconnus.
- 72% des professionnels sondés utilisent les réseaux sociaux au travail et 43% des répondants ne changent pas de mots de passe, aggravation ainsi les risques d'intrusion et de piratage.

Chiffres et évolutions des menaces II



Répartition par type des nouveaux programmes malveillants mobiles (3ème trimestre 2015 – 2ème trimestre 2016)

https://securelist.fr/it-threat-evolution-in-q2-2016-statistics/65318/

Chiffres et évolutions des menaces III

TOP 20 des programmes malveillants mobiles

Notez bien que ce classement des programmes malveillants n'inclut pas les programmes indésirables et potentiellement dangereux, tels que RiskTool ou les programmes publicitaires.

https://securelist.fr/it-threat-evolution-in-q2-2016-statistics/65318/

	Nom	% des utilisateurs attaqués*
1	DangerousObject.Multi.Generic	80,87
2	Trojan.AndroidOS.Iop.c	11,38
3	Trojan.AndroidOS.Agent.gm	7,71
4	Trojan-Ransom.AndroidOS.Fusob.h	6,59
5	Backdoor.AndroidOS.Ztorg.a	5,79
6	Backdoor.AndroidOS.Ztorg.c	4,84
7	Trojan-Ransom.AndroidOS.Fusob.pac	4,41
8	Trojan.AndroidOS.Iop.t	4,37
9	Trojan-Dropper.AndroidOS.Gorpo.b	4,3
10	Trojan.AndroidOS.Ztorg.a	4,30
11	Trojan.AndroidOS.Ztorg.i	4,25
12	Trojan.AndroidOS.Iop.ag	4,00
13	Trojan-Dropper.AndroidOS.Triada.d	3,10
14	Trojan-Dropper.AndroidOS.Rootnik.f	3,07
15	Trojan.AndroidOS.Hiddad.v	3,03
16	Trojan-Dropper.AndroidOS.Rootnik.h	2,94
17	Trojan.AndroidOS.Iop.o	2,91
18	Trojan.AndroidOS.Rootnik.ab	2,91
19	Trojan.AndroidOS.Triada.e	2,85
20	Trojan-SMS.AndroidOS.Podec.a	2,83

Plan

Cryptographie et critères de sécurité

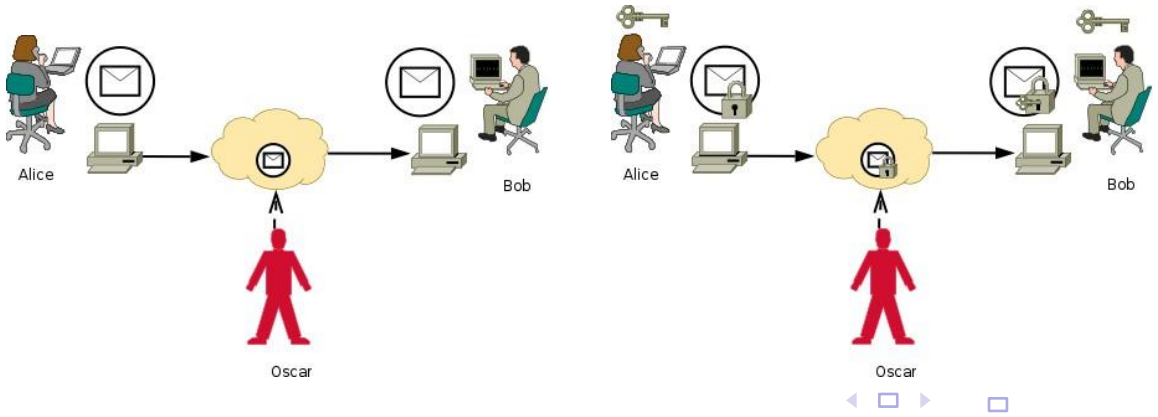
- Satisfaire les objectifs de sécurité via la cryptographie : confidentialité, intégrité, Authentification, non-répudiation, disponibilité ?
- Outils
  1. chiffrements à clé secrète partagée
  2. chiffrements à clé public
  3. signatures
  4. fonctions de hachage
- Applications : sécurité logique (données), sécurité des transmissions, sécurité de l'exploitation
- peu en sécurité applicative

Chiffrement symétrique ou à clé secrète I

Chiffrement **symétrique** ou **à clé secrète**

- confidentialité : clé secrète K partagée entre 2 personnes chiffrer :
- transforme un message clair M en un message chiffré $C = e_K(M)$ avec K
- déchiffrer : transforme un message chiffré C en un message clair $M = d_K(C)$ avec K
- algorithmes chiffrement e / déchiffrement d publics contraintes :
- difficile de déduire M de C sans K

en clair chiffré



Chiffrement symétrique ou à clé secrète II

- confidentialité des données pour une personne authentification
- de l'expéditeur si K est resté secret Exemples : DES, 3DES,
- blowfish, IDEA, AES
- Utilisés dans : SSH, SSL/TLS, WiFi (IEEE 802.11i), VPN/IPsec

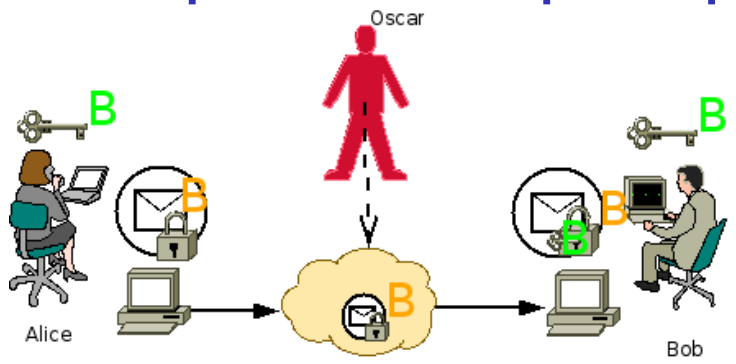
Avantages	rapidité du chiffrement/déchiffrement
Inconvénients	échange de K par un autre canal, dialogue entre n personnes nécessitent bcp de clés

Cryptographie asymétrique ou à clé publique I

Chiffrement **asymétrique** ou **à clé publique**

- confidentialité : vers tout destinataire (clé publique P, clé secrète S)
- chiffrer : message clair M en message chiffré C avec clé publique e_P
- déchiffrer : message chiffré C en message clair M avec clés $d_{P,S}$
- algorithmes chiffrement e / déchiffrement d publics
- Chiffrement asymétrique : une communication non secrète permet de véhiculer une information que seul le destinataire peut comprendre. idée [Diffie-Hellman 1976], RSA [Rivest, Shamir, Adleman 1977]
- Contrainte : difficile de déduire $d_{P,S}$ de e_P

Cryptographie asymétrique ou à clé publique II



Avantages	une seule clé secrète pour n expéditeurs, pas de canal secret
Inconvénients	lenteur, pas d'authentification de la source, attaque Man-In-The-Middle

- Très utile pour échanger les clés pour ouvrir un tunnel de communication chiffré (VPN, TLS/SSL). Uilisés aussi dans PGP.
- Nécessité de protocoles d'échanges de clé (IKE pour IPsec)
- Exemples : RSA [1977] (factorisation), chiffrement ElGamal [1985] (logarithme discret), Merkle-Hellman [1978] (sac-à-dos)

Signatures numériques I

Signature ou sceau [Diffie et Hellman (1976)]

- prouver identité de l'expéditeur (non-répudiation) et intégrité du message
- expéditeur (clé publique P, clé privée S)
- signer (privé) : fonction $sig_{P,S}$. Signature $S \leftarrow sig_{P,S}(M)$ où M est un message ou un défi
- vérifier (public) : fonction ver_P . Booléen $b \leftarrow ver_P(M,\ S)$. contraintes :
- empêcher l'usurpation, la non-reconnaissance
  - calculable par le signataire $\forall M$
  - le destinataire (et tout individu) peut vérifier la signature
  - non falsifiable
  - non imitable

- Exemple : signature RSA

Signatures numériques II

- signer $sig_{P,S}$ est le déchiffrement $d_{P,S}$

L'expéditeur donne M et $S \leftarrow sig_{P,S}(M)$.

- vérifier ver_P est le chiffrement e_P suivi d'une comparaison

Le destinataire calcule $M' \leftarrow e_P(S) = e_P(d_{P,S}(M))$ et vérifie $M = M'$

- Exemples : PGP, RSA, signature ElGamal/DSA
- Utilisation : SSL, S-MIME

Avantages	non-répudiation d'un message. En théorie, dé- coupage en blocs d'un message + signatures de chaque bloc garantit l'intégrité.
Inconvénients	Trop coûteux en pratique.

Fonctions de hachage et empreinte I

fonction de hachage et empreinte

- garantir l'intégrité d'un message M par calcul d'une **empreinte**
- hachage : message M hachée en une **empreinte** $E = h(M)$ de taille fixée
- vérification intégrité : message reçu M', $h(M') = E$? contraintes : hachage rapide, à sens unique et à collision difficile
- Exemples : MD5, SHA-1, DSA
- Utilisation : garantir l'intégrité d'une communication (SSL), de mails (S-MIME), de fichiers ou du système (antivirus)

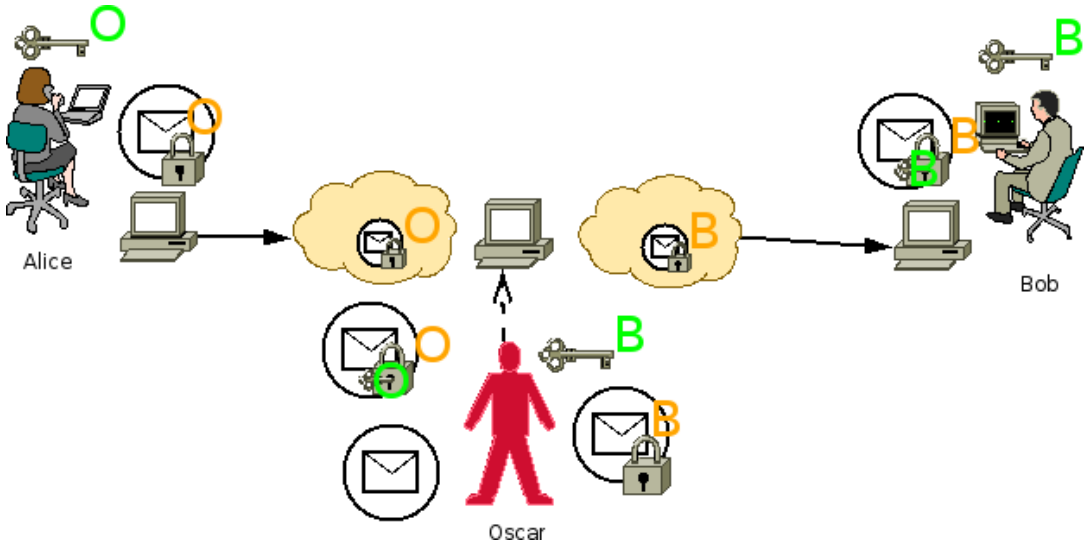
Fonctions de hachage et empreinte II

Intégrité et authentification

- message M d'un expéditeur de clés (P,S)
- signature de l'empreinte $Z \leftarrow sig_{P,S}(h(M))$
- vérification de l'intégrité par le destinataire
  1. Recevoir M^j,
  2. le hacher $h(M^j)$,
  3. puis vérifier $ver_P(h(M^j), Z) = vrai$

Authentification I

- Attaque Man-in-the-Middle (chiffrement asymétrique)



- Authentification : vérifier identité présumée d'une personne

Authentification II

Authentification par **Autorité de Certification (AC)**

- autorité de certification (AC) : organisme garant (clés P_{AC} , S_{AC})
- **légitimer** la clé publique P_A d'une personne
  1. émetteur A émet son identité Id_A et sa clé publique P_A à une AC
  2. AC vérifie l'identité de A
  3. calcule et publie un **certificat** signé par l'AC :
     $Z_{A,AC} \leftarrow sig_{P_{AC},S_{AC}}(h(Id_A, P_A))$
- authentification de A par l'utilisateur B
  1. B reçoit identifiants, clé publique de A^j
  2. compare ce qu'il reçoit : $h(Id_{A^r}, P_{A^r})$
  3. et l'autorité de certification : $ver_{P_{AC}}(h(Id_{A^r}, P_{A^r}), Z_{A,AC})$
  4. et teste l'égalité
- évite Man-in-the-Middle
- Mais quid de l'autorité de certification ?

Disponibilité I

- cryptologie : influence indirecte sur la disponibilité Contraintes fortes
- peu conciliables
  - architecture sécurisée transparente : confidentialité sans mot de passe !
  - QoS implique rapidité des mécanismes de chiffrement et déchiffrement
- Gains possibles de qualité de service :
  - en identifiant mieux les sources/demandeurs de ressource