

# Les différents aspects de la sécurité système et réseau

Christian Bulfone  
christian.bulfone@gipsa-lab.fr  
[www.gipsa-lab.fr/~christian.bulfone/IC2A-DCISS](http://www.gipsa-lab.fr/~christian.bulfone/IC2A-DCISS)



Master IC2A/DCISS  
Année 2011/2012

## Plan du cours

- Les risques
- Le chiffrement des informations
- Sécurité informatique
- Programmation C, Shell ...
- Les firewalls
- Quelques exemples d'attaques

## Sources d'information



- Sécurité
  - <http://www.linuxsecurity.com>
  - <http://www.infosyssec.org>
  - <http://www.securityfocus.com>
  - <http://www.seifried.org/lasg> (*Linux Administrator's Security Guide*)
  - <http://www.hsc.fr/ressources/breves>
- Cryptologie
  - <http://www.commentcamarche.net/crypto/crypto.php3>
  - <http://www.bibmath.net/crypto/index.php3>
  - <http://www.apprendre-en-ligne.net/crypto>
  - <http://www.openssh.org>

## Sources d'information

- Le CERT : <http://www.cert.org>
- Recense les problèmes de sécurité par :
  - Alertes
  - Vulnérabilités
  - Informations
  - Statistiques
- Les pirates sont aussi à l'écoute de ces informations !
- Permet de se tenir au courant en permanence et de réagir vite en cas de problème
- Possibilité de s'abonner aux listes de diffusion
- Autres sources :
  - CIAC (Computer Incident Advisory Capability) : <http://www.ciac.org/ciac/>
  - SANS (System Administration, Networking, and Security) : <http://www.sans.org>

## Dispositions légales

- Le chapitre III du Code pénal traite des atteintes aux Systèmes de Traitement Automatisé de Données (STAD)
  - **L'article 323-1** condamne le fait d'accéder et se maintenir frauduleusement, c'est-à-dire sans droits, dans un système. Les peines vont jusqu'à 3 ans de prison et 45 000 € d'amende
  - **L'article 323-2** sanctionne le fait d'entraver ou de fausser le fonctionnement d'un STAD de 5 ans de prison et de 75 000 € d'amende
  - **L'article 323-3** condamne le fait d'introduire frauduleusement des données ou supprimer ou modifier frauduleusement des données. Le délit est puni de 5 ans de prison et 75 000 € d'amende.
  - **L'article 323-3-1** condamne le fait de détenir ou d'offrir des moyens permettant les délits cités dans les articles 323-1 à 323-3 et sanctionne de la même manière que les délits
  - **Les articles 323-4 à 323-7** sanctionnent la préparation des délits, l'intention, prévoient des peines complémentaires telles qu'interdiction des droits civiques, civils, de famille, d'exercer dans la fonction publique, la fermeture des établissements ayant servi à commettre les faits, des sanctions pour les personnes morales.

## Les risques

- Quoi protéger ?
  - Les données
    - protection contre le risque de divulgation
    - protection contre l'altération ou la perte d'informations
    - protection contre la dégradation
  - Les ressources
    - serveur, disques, imprimantes, réseau, ...
      - protection contre le refus de service
  - La réputation de l'entreprise et des personnes
    - usurpation d'identité, ...

## Origines des risques

- Risques accidentels
  - Risques matériels accidentels (incendie, explosion, chocs, collision, inondation ...)
  - Vol et sabotage
  - Panne et dysfonctionnement de matériel ou de logiciel de base
- Risques d'erreur
  - Erreur de saisie, de transmission
  - Erreur d'exploitation
  - Erreur de conception et de réalisation
- Risques de malveillance
  - Fraude, sabotage immatériel
  - Indiscrétion (jusqu'à l'espionnage industriel ou commercial), détournement d'informations
  - Détournement de logiciels (piratage)
  - Grève, départ de personnel stratégique

## Les attaques

- Vol d'informations
  - attaque passive (écoute du réseau),
  - *social engineering*
    - ensemble de techniques utilisées pour extorquer à un individu toute information utile facilitant l'intrusion dans un système (mot de passe, code confidentiel ...)
- Intrusion
  - prise de contrôle partielle ou totale d'un système distant
  - la plus connue et la plus pratiquée,
  - rendue possible par des problèmes d'authentification, trous de sécurité du système ...
- Refus (dédi) de service
  - empêcher l'utilisation des machines, du réseau ...
  - inondation de processus, de messages, de requêtes, ...

## Les dénis de service (DoS)

- Attaques aboutissant à l'indisponibilité du service ou de la machine visée
- Deux types :
  - dénis de service **applicatifs**
    - exploitation des vulnérabilités d'une application : débordement de buffer (*buffer overflow*) par exemple
    - indisponibilité par saturation des ressources ou par crash de l'application
  - dénis de service **réseaux**
    - exploitation des faiblesses d'un protocole
    - exploitation de la mauvaise implémentation d'un protocole

## Description d'une attaque type

- Recherche d'informations
  - réseau, routeurs, serveurs ...
- Recherche de vulnérabilités
  - systèmes d'exploitation, applicatifs ...
- Tentatives d'exploitation des vulnérabilités
  - A distance / localement
- Mise en place de portes dérobées (*backdoor*), de systèmes d'écoute du réseau (*sniffer*)
- Suppression des traces
- Attaque par déni de service

## Techniques de recherche d'information

- Recherche d'informations publiques
  - interrogation DNS, whois, moteurs de recherche
- Découverte
  - de la topologie du réseau et du filtrage IP en place
    - `tracert`, `ping`, `hping`, `firewalk`, `filterrules`
  - des systèmes d'exploitation
    - outils de prise d'empreinte
    - `nmap`
  - des services ouverts
    - outils de scan de ports
    - `strobe`, `nmap`, `udp-scan`
  - des versions logicielles
    - faire afficher les bannières des programmes
    - `telnet`, `netcat`

## La sécurité informatique

- Consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu
- Le terme « sécurité » recouvre 3 domaines
  - La **fiabilité** de fonctionnement
    - S'exprime en terme de disponibilité
  - La **confidentialité** de l'information
    - Consiste à s'assurer que seules les personnes autorisées aient accès aux ressources
  - L'**intégrité** des données
    - Confidentialité et intégrité font appel aux techniques de la **cryptographie**

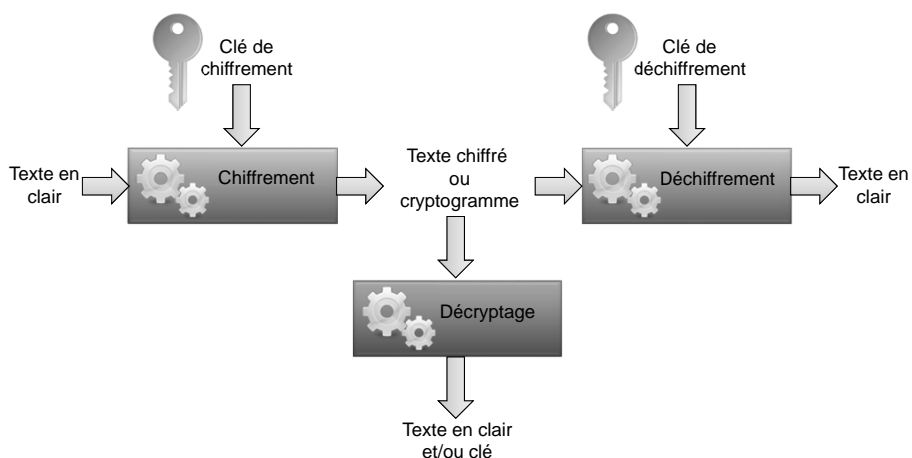
# Authentification

- Processus par lequel une entité (personne, machine ...) **prouve son identité**
- Plusieurs classes de méthodes d'authentification possibles
  - « je connais »
    - exemple du mot de passe
    - pas d'authentification sans une **identification** préalable (login)
  - « je possède »
    - exemple de la carte magnétique
  - « je suis »
    - exemple de l'empreinte digitale (biométrie)
  - « je sais faire »
    - exemple de la signature manuscrite



# Le chiffrement des informations

- Cryptologie = cryptographie + cryptanalyse
- Chiffrement, déchiffrement, décryptage



## Le chiffrement des informations

- La cryptographie réalise plusieurs fonctions :
  - **Confidentialité** : consiste à rendre l'information inintelligible à des personnes autres que les acteurs de la transaction
  - **Intégrité** : consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle)
  - **Authentification** : a pour but de vérifier l'identité dont une entité se réclame ; cela permet de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être

## Les cryptosystèmes

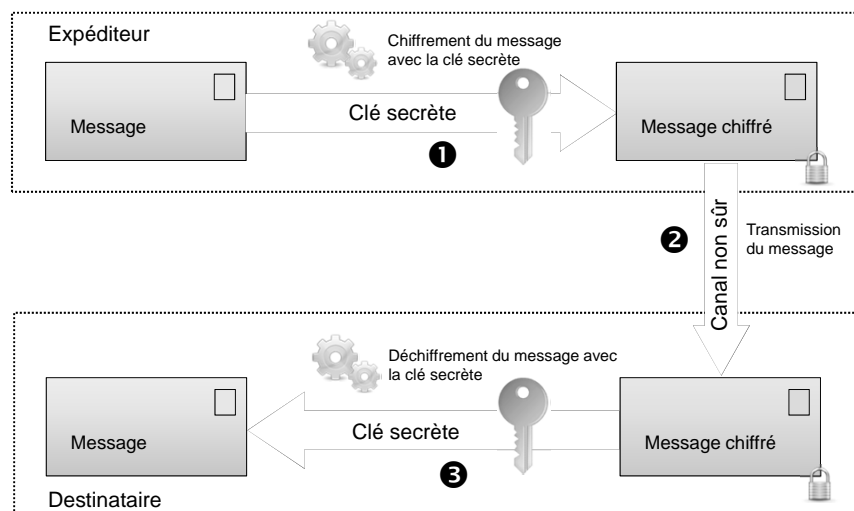
- Cryptosystème à usage restreint
  - basé sur la confidentialité des algorithmes de chiffrement et de déchiffrement
  - inutilisable avec beaucoup d'utilisateurs
  - confidentialité non assurée
- Cryptosystème à usage général
  - algorithmes éventuellement secrets mais pas nécessairement
  - utilisation de clés pour chiffrer et déchiffrer
  - nécessite un grand nombre de clés pour éviter que l'on puisse réaliser une recherche exhaustive sur les clés



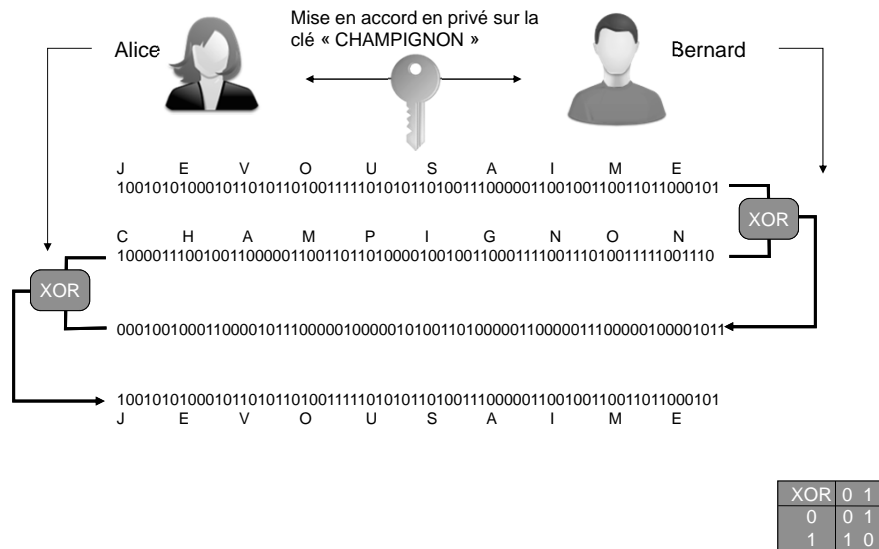
## Le chiffrement symétrique

- Cryptographie à clé secrète (chiffrement symétrique)
  - une **même clé secrète** pour le chiffrement et le déchiffrement du message
  - pour que le système soit sûr, la longueur de la clé doit être au moins égale à celle du message à chiffrer
  - nécessite d'utiliser un **canal sûr** pour se transmettre la **clé**
  - si chaque paire parmi N utilisateurs partagent une clé, il faut alors  $N^2$  clés secrètes

## Le chiffrement symétrique



## Principe de fonctionnement



## Problème de l'échange des clés

- Chaque participant doit posséder une copie de la clé : comment s'échanger cette clé de façon sécurisée ?
- Problème d'autant plus épineux si
  - La clé doit être changée souvent
  - Le nombre de communicants devient élevé
  - Un des participants n'est pas honnête
- C'est au début des années 70 que la solution fut trouvée !

## Comment partager un secret ?

- Paradoxe de la cryptographie à clé privée : pour que deux personnes puissent communiquer secrètement, elles doivent déjà partager un secret !
- Exemple du facteur
  - On suppose que Alice veut envoyer un colis secret à Bernard par la poste, mais que leur facteur ne peut s'empêcher de lire les correspondances non closes
  - Comment peut-elle le lui envoyer ?

## Comment partager un secret ?

- Solution
  - Alice met son colis dans une boîte qu'elle ferme avec un cadenas et l'envoie à Bernard
  - Bernard reçoit le colis, rajoute un cadenas à la boîte et renvoie le tout à Alice
  - Alice retire son cadenas avec sa clé et renvoie la boîte à Bernard
  - Bernard peut maintenant ouvrir la boîte avec sa clé et profiter du colis
- Remarque
  - A aucun moment le facteur n'a été en mesure d'ouvrir la boîte

## Exemple sur des nombres

- On considère qu'Alice veut envoyer le nombre 15 à Bernard
  - Alice choisit d'abord un nombre au hasard, par exemple 22
  - Elle envoie la somme des deux nombres à Bernard
  - Bernard reçoit le nombre 37
  - A son tour il choisit un nombre au hasard, par exemple 18 et renvoie la somme des deux nombres à Alice
  - Alice reçoit le nombre 55
  - Elle soustrait son nombre secret et envoie le résultat à Bernard
  - Bernard soustrait enfin son nombre secret et obtient le message d'Alice

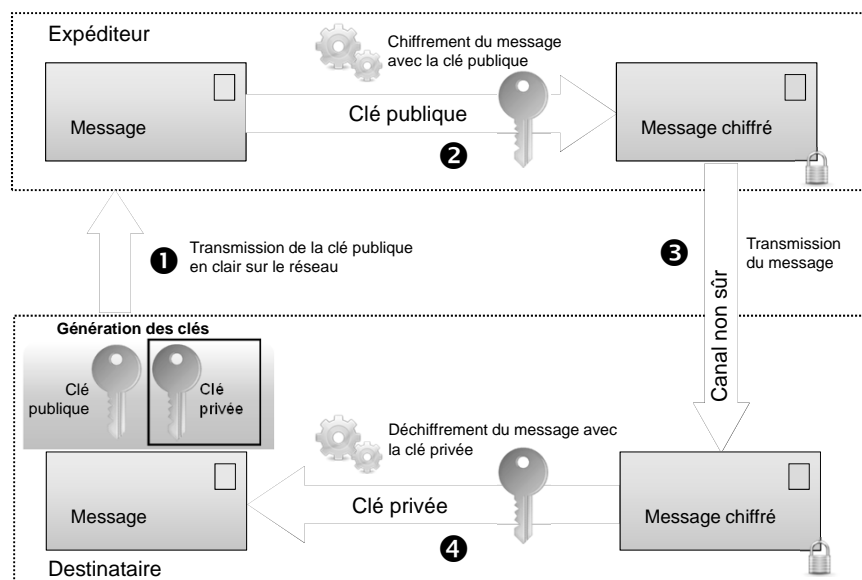
## Principe de la cryptographie asymétrique

- Utilise des fonctions mathématiques faisant offices de cadenas
  - Faciles à utiliser dans un sens
  - Très difficile à inverser à moins de connaître un paramètre secret
- Problème de la factorisation des nombres premiers
  - Facile dans un sens
    - $13 \times 17 = 221$
    - $10\,247 \times 17\,159 = 175\,828\,273$
  - Difficile dans l'autre
    - $209 = 11 \times 19$
    - $7\,321\,010\,267 = 55\,487 \times 131\,941$

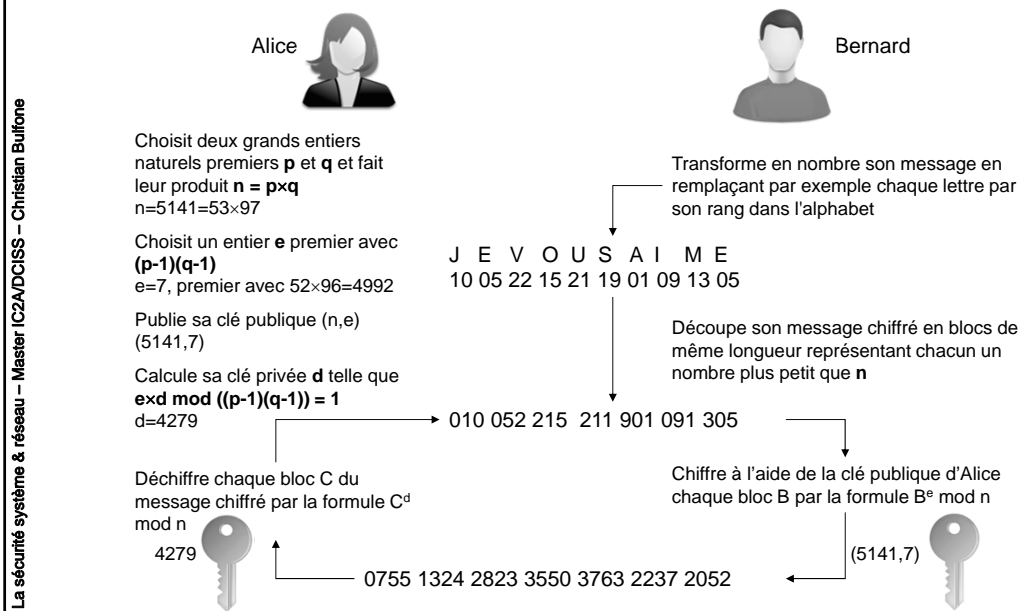
## Le chiffrement asymétrique

- Cryptographie à clé publique (chiffrement asymétrique)
  - une **clé pour chiffrer**, une **clé pour déchiffrer**
  - le message est chiffré avec la clé publique du destinataire
  - seule la clé privée peut déchiffrer le message chiffré
  - seul le destinataire possède et connaît la clé privée
  - il est impossible de calculer la clé privée à partir de la clé publique

## Le chiffrement asymétrique

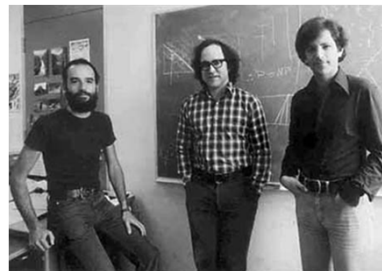


## Principe de fonctionnement



## RSA, 1er protocole à clé publique

- 1975
  - Diffie, Hellman et Merkle inventent le principe de la cryptographie à clé publique
  - Mais aucun exemple concret n'est proposé
- 1977
  - Ronal Rivest, Adi Shamir et Leonard Adleman inventent le premier protocole de cryptographie à clé publique : RSA
  - Basé sur le problème de la factorisation



## Challenge RSA

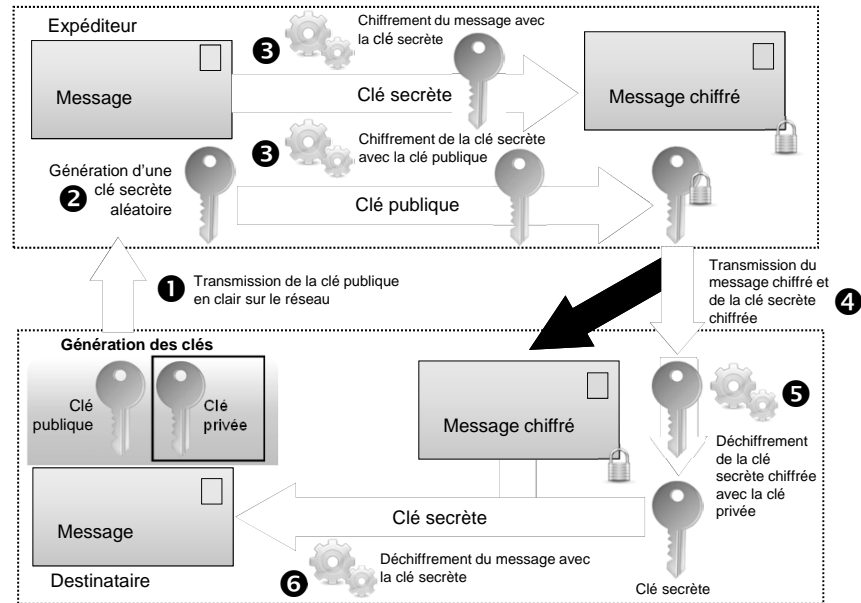
- RSA fut présenté en 1977 dans le magazine Scientific American, accompagné d'un concours :
- Factoriser le nombre  
114 381 625 757 888 867 669 235 779 976 146 612  
010 218 296 721 242 362 562 561 842 935 706 935  
245 733 897 830 597 123 563 958 705 058 989 075  
147 599 290 026 879 543 541  
et utiliser cette factorisation pour déchiffrer un message codé avec RSA  
100\$ était offert au premier qui parviendrait à déchiffrer le message
- Il aura fallu 17 ans pour qu'une équipe de 600 personnes remporte le concours

## La clé de session

- Cryptographie à clé mixte
  - les algorithmes asymétriques sont généralement lents
  - les algorithmes symétriques sont plus rapides, mais posent le problème de l'échange des clés
  - la clé de session offre un compromis entre le chiffrement symétrique et asymétrique en combinant les deux techniques
    - une clé secrète (clé de session) de **taille raisonnable** est générée aléatoirement puis chiffrée à l'aide de la clé publique du destinataire
    - le destinataire déchiffre la clé secrète à l'aide de sa clé privée
    - l'émetteur et le destinataire possèdent tous deux la clé secrète pour chiffrer et déchiffrer les messages échangés au cours de la session
    - la session terminée, la clé symétrique est détruite

## La clé de session

La sécurité système & réseau – Master IC2A/DCISS – Christian Bulfone



## Des clés de tailles différentes ?

La sécurité système & réseau – Master IC2A/DCISS – Christian Bulfone

- La sûreté d'une **clé secrète** dépend de sa longueur
  - Avec une clé de
    - 1 bit, on a  $2^1 = 2$  possibilités (0, 1)
    - 2 bits, on a  $2^2 = 4$  possibilités (00, 01, 10, 11)
    - 3 bits, on a  $2^3 = 8$  possibilités (000, 001, 010, 011, 100, 101, 110, 111)
    - 56 bits, on a  $2^{56} = 72\,057\,594\,037\,927\,936$  possibilités
  - Pour **chaque bit** ajouté, le nombre de possibilités **double** !
- Pour casser une clé secrète, il faudra essayer toutes les combinaisons possibles
- Compte tenu de la puissance de calcul des ordinateurs actuels, la taille des clés secrètes **ne doit pas être inférieure à 128 bits**
  - Jusqu'en 1998, la taille des clés autorisées en France n'était que de 40 bits !
  - La même année, les clés de 56 bits étaient cassées

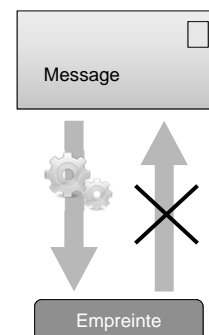


## Des clés de tailles différentes ?

- Les clés des systèmes asymétriques sont différentes
  - Utilisent des nombres premiers
    - Il est facile de multiplier les deux nombres premiers 127 et 997 et de trouver 126 619
    - Mais il est plus difficile de retrouver 127 et 997 à partir de 126 619
  - Casser une clé asymétrique revient donc à rechercher le produit des nombres premiers d'un nombre
  - Si ce nombre est très grand, cette recherche est impossible dans un temps raisonnable
  - Actuellement, les clés ne doivent pas être inférieures à 1024 bits

## Intégrité des données

- Fonction de hachage
  - Convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe = empreinte ou condensé
  - A sens unique
    - Facile à calculer mais difficile à inverser
    - Il est difficile de trouver deux messages ayant la même empreinte
  - MD5 (*Message Digest 5*)
    - Empreinte de 128 bits
  - SHA (*Secure Hash Algorithm*)
    - Empreinte de 160 bits



## Les protocoles SSH / SSL

- Plusieurs protocoles peuvent être utilisés pour chiffrer et authentifier les échanges
  - SSH (*Secure SHell*)
    - Il s'agit à la fois de la définition d'un protocole et d'un ensemble de programmes permettant
      - des sessions interactives depuis une machine cliente à distance sur des serveurs
      - de transférer des fichiers entre deux machines de manière sécurisée
    - ces programmes ont pour but de remplacer les utilitaires de connexions classiques n'utilisant pas de chiffrement (`rlogin`, `rsh` et `telnet` notamment)
    - SSH chiffre et compresse un tunnel de session évitant ainsi la circulation des mots de passe et des données en clair sur le réseau

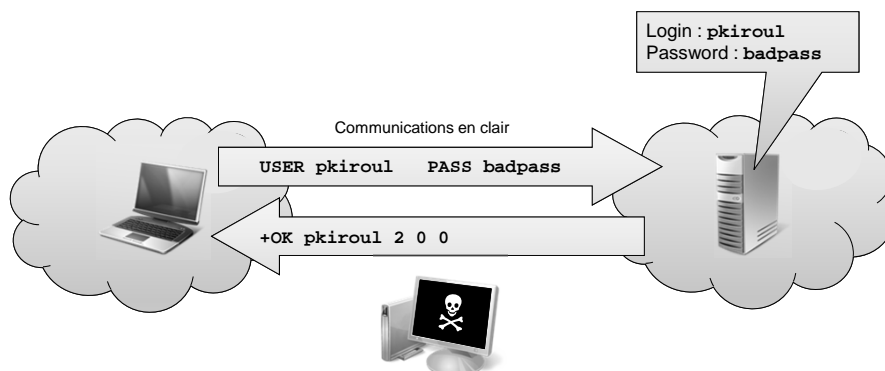
## Les protocoles SSH / SSL

- Deux modes d'authentification de l'utilisateur peuvent être mis en oeuvre avec SSH
  - une **authentification "traditionnelle"** par mot de passe
    - comme le canal est déjà chiffré par le protocole SSH, le mot de passe en clair est encapsulé dans une communication secrète
  - une **authentification forte**
    - l'authentification est basée sur la cryptographie asymétrique, utilisant des clés publique/privée
    - la clé privée est protégée par une *passphrase*
    - cette passphrase ne circule pas sur le réseau
    - l'utilisateur s'identifie alors sans utiliser le mot de passe de la connexion classique (mot de passe Unix), mais à l'aide de ces clés (et de sa passphrase pour accéder à sa clé privée)

## Les protocoles SSH / SSL

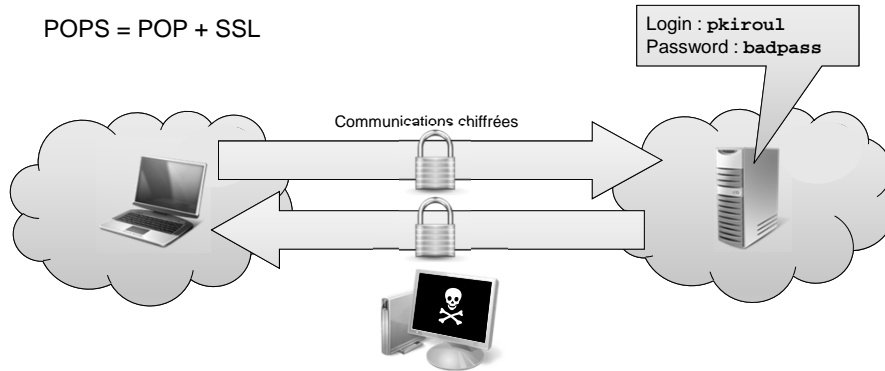
- SSL (*Socket Secure Layer*)
  - protocole mis en oeuvre initialement par Netscape et repris par l'IETF sous le nom TLS (*Transport Layer Security*)
  - offre un certain nombre de services de sécurité tels que la confidentialité des données transmises ou l'authentification des interlocuteurs à l'aide de certificats électroniques
  - SSL est utilisé pour sécuriser des services Web (protocole HTTPS), ou encore des protocoles comme POP et IMAP (on parle alors des protocoles POPS et IMAPS)

## La relève du courrier avec POP



## La relève du courrier avec POPS

POPS = POP + SSL



La sécurité système & réseau – Master IC2A/DCISS – Christian Buftone

## Les OTP

- Systèmes à mot de passe unique (*One Time Password*)
  - un nouveau mot de passe à chaque nouvelle connexion
  - rend inutile la capture du mot de passe (en clair) sur le réseau
  - initialisation du mot de passe secret sur le serveur en local
  - le serveur envoie un challenge lors de la connexion
  - calcul du OTP en utilisant une calculatrice (sans utiliser le réseau !)
    - challenge + mot de passe secret = OTP

La sécurité système & réseau – Master IC2A/DCISS – Christian Buftone

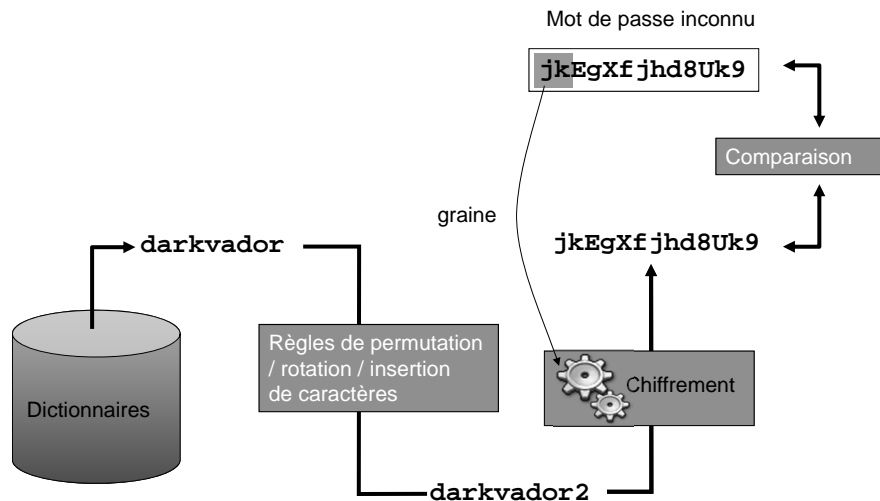
## Politique de sécurité

- Ensemble des orientations suivies par une organisation (au sens large) en terme de sécurité
- Se doit d'être élaborée au niveau de la **direction** de l'organisation concernée
- Doit être abordée dans un **contexte global**
  - Au niveau des utilisateurs
    - Sensibilisation aux problèmes de sécurité
  - Au niveau des applications
  - Au niveau des données
  - Au niveau des télécommunications
  - Au niveau des infrastructures matérielles

## Sécurité des comptes utilisateur

- Choix du mot de passe très important
- Un « bon » mot de passe :
  - doit contenir au moins 8 caractères alphanumériques mélangeant majuscules, minuscules et caractères de ponctuation
  - ne doit pas être basé sur un nom commun, un nom propre ... qui peut être présent dans un dictionnaire français ou étrangers
- Il existe des outils (*cracker*) pour éprouver la « solidité » d'un mot de passe
  - cracker systématique sur un PIII 700 MHz :
    - 2 lettres en moins de 1 seconde
    - 3 lettres en moins de 20 secondes
    - 4 lettres en environ 30 minutes
    - beaucoup moins de temps sur une machine parallèle ...
    - mais beaucoup plus avec des mots de passe longs et en MD5
  - cracker à dictionnaires

## Principe du *crackage* par dictionnaires



## Sécurité Unix : root

- Interdire le login à distance de root
  - efficace si l'accès physique à la machine est protégé
  - utilisation de la commande **su**
- Bien découper les groupes pour répartir les droits
- Ouverture de certaines commandes avec **sudo**
- SUID & SGID
  - possibilité d'endosser les droits du propriétaires pendant l'exécution de programme
  - **jamais de SUID root** sur un shell script !!!

## Sécurité Unix : root

La sécurité système & réseau – Master IC2A/DCISS – Christian Bulfone

- Le noyau est accessible à travers le fichier `/proc/kcore` (seulement en lecture pour root !)
- Le répertoire courant dans le PATH
  - `PATH = /bin:/usr/bin:/usr/local/bin:.`
  - `PATH = ./bin:/usr/bin:/usr/local/bin`
  - Que peut-il se passer si je fais `cp /bin/rm ~cheztoi/ls`
- Toujours utiliser des paths absolus dans les shells-scripts :
  - `system("/bin/ls")`
  - `system("ls")` à éviter absolument !

## Programmation

La sécurité système & réseau – Master IC2A/DCISS – Christian Bulfone

- Ne jamais faire confiance aux programmes extérieurs
- Exemple :

```
main(int argc, char *argv[]) {  
    ...  
    system(argv[1]);  
}
```

```
-rwsr-xr-x 1 root sys 2001 Dec 25 00:59 monprog
```
- On peut facilement se créer un compte root avec ce programme :

```
monprog "echo 'cbulfone::0:0:::/bin/bash' > /etc/passwd"  
su cbulfone
```

## Programmation

- En programmation réseau, il ne faut jamais faire confiance aux informations reçues
  - L'utilisateur peut envoyer plus de données que celles qu'il a annoncé
- Attaque par débordement de buffer (*buffer overflow*)
  - Exemple typique
 

```
int fonction (char *param) {
    char tableau[256];
    gets(tableau);
    return strcmp(tableau, param);
}
```
  - Si l'utilisateur entre plus de 256 caractères, il peut modifier les données dans la pile !!!
- Toujours utiliser des fonctions qui permettent de vérifier la taille des buffers

## Configuration réseau

- Adresses IP
  - définition manuelle plutôt que dynamique
  - tables ARP statiques pour éviter l'usurpation d'adresse IP
- Routage
  - routes statiques pour éviter la prise en compte de fausses routes reçues par un démon de routage
  - éviter les routes par défaut
- Routeurs filtrants
  - possibilité d'effectuer du filtrage sur les connexions
  - adresses IP, protocoles (TCP, UDP), numéros de port



## Le firewall



- Dénommé *garde barrière, coupe-feu, pare-feu* ...
- Permet de restreindre l'accès au réseau en un point précis
- Empêche les agresseurs de s'approcher des autres défenses

Ce que peut faire un firewall	Ce que ne peut pas faire un firewall
<ul style="list-style-type: none"><li>• Centraliser les décisions de sécurité</li><li>• Renforcer la sécurité des services Internet proposés</li><li>• Déterminer une réglementation d'accès vers et depuis l'Internet</li><li>• Isoler une partie du réseau</li><li>• Contrôler et enregistrer l'activité Internet</li></ul>	<ul style="list-style-type: none"><li>• Protéger les connexions qui ne passent pas par le firewall</li><li>• Protéger contre les menaces totalement nouvelles</li><li>• Protéger contre les virus</li><li>• Se protéger des utilisateurs internes malveillants</li></ul>

## Classification des firewalls

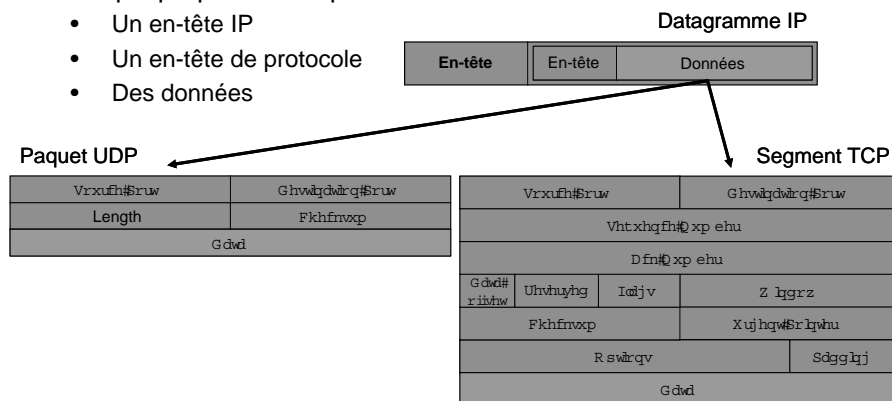
- Plate-forme logicielle
  - Peut être mis en œuvre sur un simple PC avec plusieurs interfaces réseau, embarquant un OS généraliste (Linux, ou un autre UNIX)
  - Les fonctions du pare-feu sont implémentées à l'aide d'un logiciel adapté
    - Ipchains ou Netfilter sous Linux ; Packet Filter sous OpenBSD
- Firewall matériel
  - Se présente sous la forme d'un boîtier spécialisé embarquant un OS souvent minimaliste
    - Routeurs : le contrôle des flux entrants et sortants est réalisé à l'aide de filtres (*access-lists*)
    - Equipements dédiés : conçus uniquement pour agir en tant que pare-feu, avec les niveaux de performances nécessaires

## Les fonctions d'un firewall

- Un pare-feu assure un ensemble de fonctions
  - Le **filtrage**
    - Il s'agit de la principale fonction
  - L'**authentification** des utilisateurs et la **gestion des droits**
    - Protocoles d'authentification RADIUS ou TABACS+
  - La **translation d'adresses** ou **NAT** (*Network Address Translation*)
    - Permet d'occulter totalement le plan d'adressage interne de l'entreprise et de réduire le nombre d'adresses IP officielles nécessaires

## Le filtrage IP

- Les services Internet ou Intranet sont basés sur IP
- Tout protocole IP repose sur des datagrammes IP
- Chaque paquet IP comprend des informations
  - Un en-tête IP
  - Un en-tête de protocole
  - Des données



## Le filtrage IP

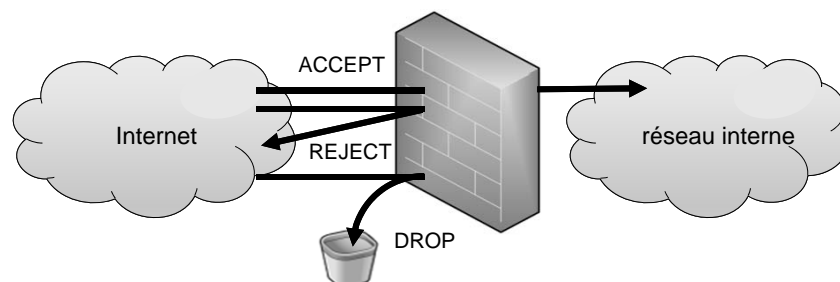
- Chaque protocole IP peut s'identifier
  - De manière générale
  - Au niveau de chaque communication
- Pour chaque paquet IP, on peut
  - Accepter ou router le paquet (ACCEPT)
  - Rejeter le paquet (DROP/REJECT)
  - Détourner le paquet vers un autre service (REDIRECT)
- Deux politiques possibles :
  - « Ce qui n'est pas explicitement interdit est autorisé »
  - « Ce qui n'est pas explicitement autorisé est interdit »



La politique la plus restrictive est toujours la plus sûre !

## Le filtrage IP

- **ACCEPT**
  - Tous les paquets sont acceptés
- **DROP**
  - Les paquets sont refusés sans notification à l'émetteur des paquets
- **REJECT**
  - Les paquets sont refusés mais avec notification (ICMP) à l'émetteur des paquets



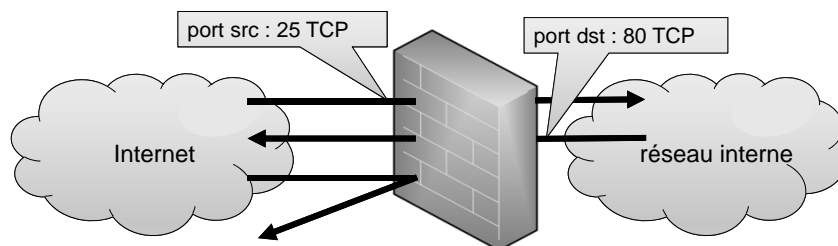
## Le filtrage IP

- Technologie de filtrage simple (*stateless*)
  - autorise ou interdit le passage des paquets en se basant sur des critères tels que :
    - le type de protocole IP (ICMP, TCP, UDP ...)
    - les ports TCP/UDP source ou destination
    - les adresses IP source ou destination
- Technologie de filtrage *stateful*
  - agit comme un filtre de paquets simple mais garde une trace de tout échange de données soumis à son approbation
  - adapte son comportement en fonction de cet état

## Filtrage stateless

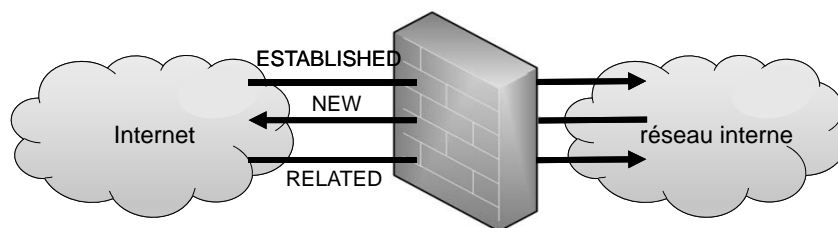
- Le filtrage ne prend pas en compte l'état du paquet

```
access-list 101 permit tcp any eq 25 host 195.83.80.5
access-list 102 permit tcp any any eq 80
access-list 101 deny ip any any log
```



## Filtrage stateful

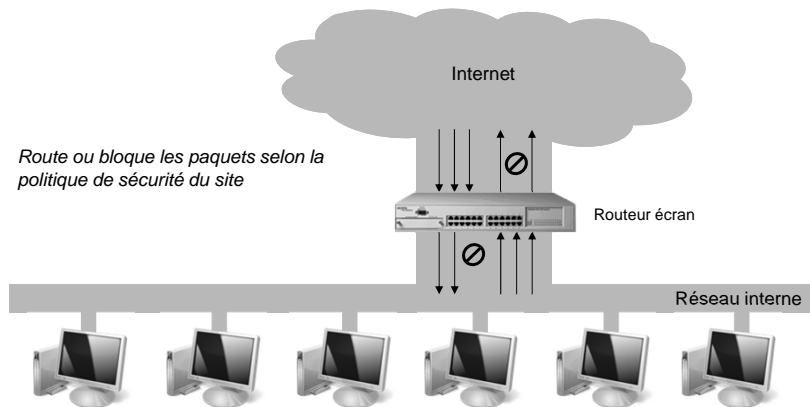
- Le filtrage prend en compte l'état du paquet
  - ESTABLISHED
    - Paquet associé à une connexion déjà établie
  - NEW
    - Paquet demandant une nouvelle connexion
  - INVALID
    - Paquet associé à une connexion inconnue
  - RELATED
    - Nouvelle connexion mais liée



## Les services à filtrer

- Les principaux services à protéger :
  - le courrier électronique (SMTP TCP/25, POP3 TCP,UDP/110),
  - le transfert de fichiers (FTP TCP/21, TFTP UDP/69, SFTP TCP/115),
  - l'accès par terminal (Telnet TCP/23) et l'exécution de commandes à distance,
  - le World Wide Web (HTTP TCP,UDP/80),
  - les services de conférence en temps réel,
  - le service de nom (DNS, TCP,UDP/53),
  - les services d'administration réseau (SNMP UDP/161,162),
  - les services temporels (NTP TCP,UDP/123),
  - les systèmes de fichiers réseau (NFS sur RPC TCP,UDP/111, SMB TCP,UDP/137-139,445),
  - les services d'impression (printer TCP/515)

## Firewall à routeur écran

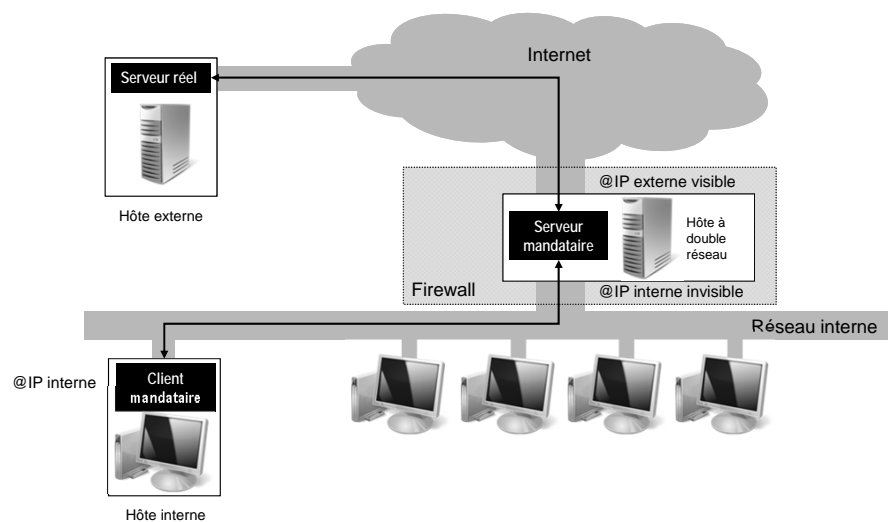


## La translation d'adresses (*IP masquerading*)

- Les paquets venant de réseaux privés ne sont pas routables
  - Les adresses IP privées sont définies dans la RFC 1918
    - classe A : 10.0.0.0 à 10.255.255.255
    - classe B : 172.16.0.0 à 172.31.255.255
    - classe C : 192.168.0.0 à 192.168.255.255
- Une passerelle (ou *proxy*) fait la liaison réseau privé ↔ Internet
- Les paquets venant des hôtes du réseau privé sont réécrits (camouflés ou masqués) lorsqu'ils passent par la passerelle, comme s'ils provenaient de la passerelle elle-même
- Les réponses à destination des hôtes du réseau privé sont réécrites par la passerelle, comme si elles venaient du destinataire originel

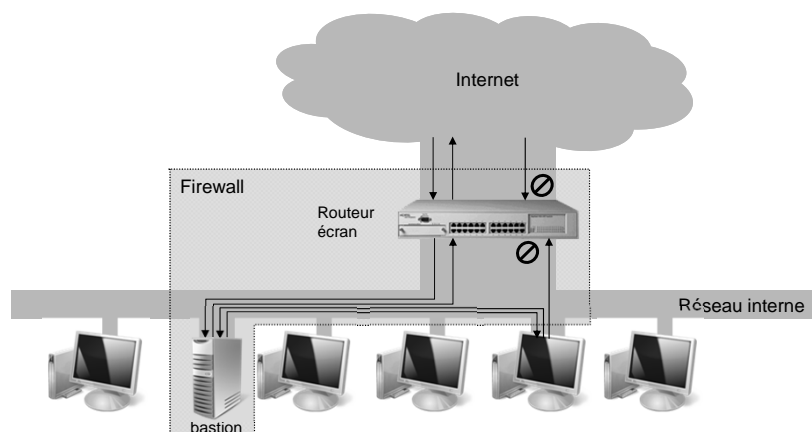
## Firewall à proxy

La sécurité système & réseau – Master IC2A/DCISS – Christian Buifone

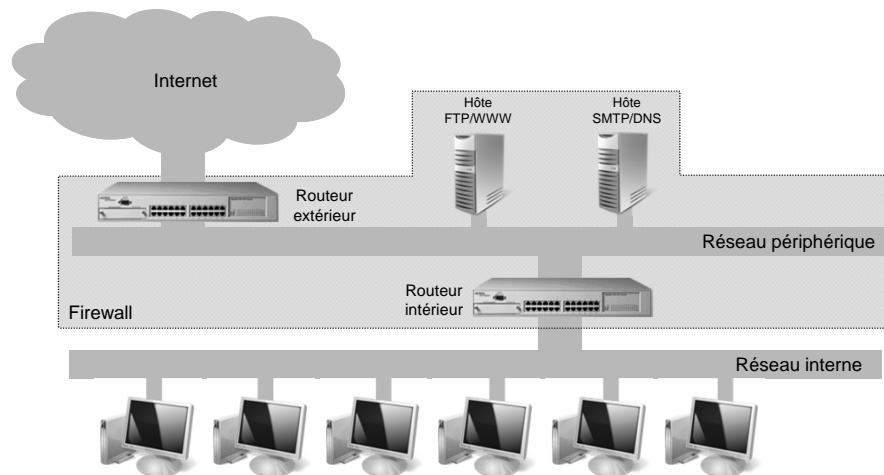


## Firewall avec bastion

La sécurité système & réseau – Master IC2A/DCISS – Christian Buifone

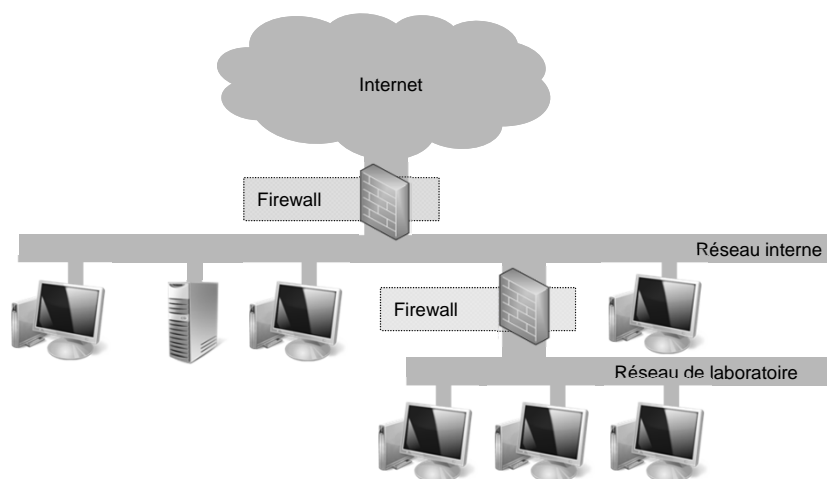


## Firewall à zone démilitarisée



La sécurité système & réseau – Master IC2A/DCISS – Christian Buflone

## Firewalls hiérarchiques



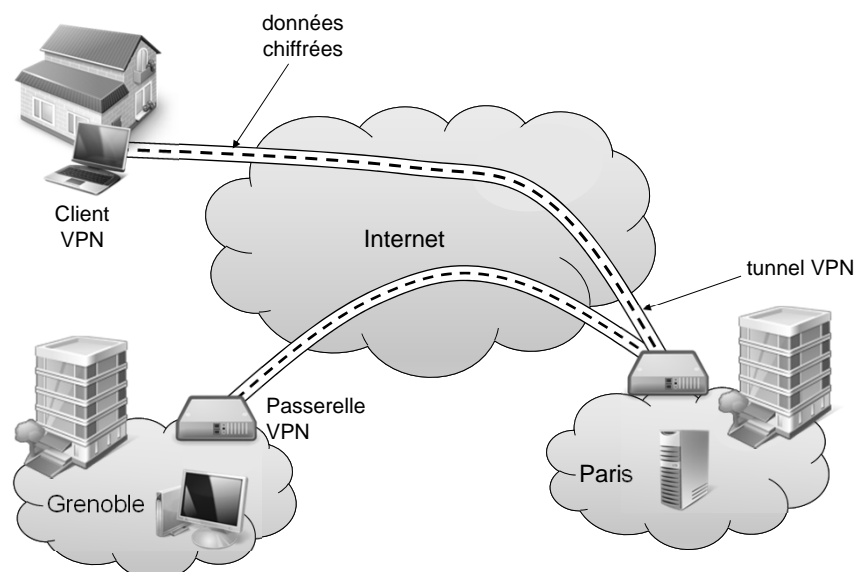
La sécurité système & réseau – Master IC2A/DCISS – Christian Buflone



## Réseau privé virtuel VPN (*Virtual Private Network*)

- Réseau privé virtuel (RPV) ou *Virtual Private Network* (VPN)
  - virtuel
    - relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet)
  - privé
    - seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent « voir » les données
- Repose sur un protocole d'encapsulation (*tunneling*)
  - Les données sont chiffrées entre l'entrée et la sortie du VPN comme si elles passaient dans un tunnel
  - IPSec est le protocole d'encapsulation utilisé pour les réseaux IP

## Réseau privé virtuel VPN (*Virtual Private Network*)



## Sécurité des réseaux sans fil

1. Gérer les WLAN
2. Utiliser la sécurité des bornes
3. Mettre en place un mécanisme de chiffrement
4. Architecturer correctement les WLAN

## Gérer les WLAN

- Doit être réalisée par une équipe formée et compétente
- Les bornes sans fil doivent être gérées comme des équipements sensibles assurant des fonctions de sécurité
- Ajouter les réseaux sans fil dans la sensibilisation des utilisateurs à la sécurité
- Faire des audits réguliers
  - Surveiller le trafic
  - Rechercher les réseaux sans fil sauvages
- Intégrer les problématiques des réseaux sans fil dans sa politique de sécurité et ses procédures

## Utiliser la sécurité des bornes

- Gérer et superviser des bornes uniquement par l'interface filaire
- Désactiver tous les services d'administration sur l'interface sans fil
  - Interface Web
  - SNMP
  - TFTP
- Modifier les paramètres de configuration par défaut
  - SSID
  - Clé WEP
  - Noms de communauté SNMP
- Choisir des mots de passe forts
  - Sans lien avec le réseau ou l'entreprise

## Utiliser la sécurité des bornes

- Mettre à jour son firmware régulièrement
- Mettre en place un filtrage par adresse MAC
  - Seules les cartes enregistrées sont autorisées à utiliser le réseau
    - Gestion quotidienne lourde
    - L'adresse MAC figure en clair dans tous les trames, même si WEP est employé
    - Possibilité d'écouter le trafic pour repérer les adresses MAC valides
    - Génération de trames falsifiées avec une adresse MAC valide

## Mettre en place un mécanisme de chiffrement

- WEP (Wired Equivalent Privacy)
  - Premier mécanisme de sécurité mis en place dans 802.11
    - Concerne la grande majorité des équipements actuels
    - Utilise des clés secrètes partagées de 64 ou 128 bits
      - Tout le monde possède la même clef
    - Basé sur l'algorithme de chiffrement par flot RC4
      - Problème d'initialisation
    - Pas de gestion des clefs
      - Les clefs sont configurées et déployées manuellement
      - Rarement changées
- WPA (WiFi Protected Access)
  - Solution de transition en attendant 802.11i
  - Basé sur un nouveau protocole de gestion des clés : TKIP
  - Permet de générer et distribuer des clés WEP

## Architecturer correctement ses WLAN

- Considérer les bornes 802.11 comme des équipements sensibles
  - Choisir des bornes dont le firmware peut être mis à jour
    - Correctifs de sécurité
    - Nouvelles fonctionnalités
- Prendre en compte la sécurité des ondes dans l'espace
  - Choisir consciencieusement l'emplacement des bornes ou des antennes
  - Régler la puissance des bornes au plus juste
- Considérer les flux 802.11 comme des flux extérieurs (ie Internet)
  - Les bornes doivent être placées derrière une passerelle
  - Les flux doivent être filtrés au niveau de la passerelle
  - Les utilisateurs doivent être authentifiés

## Exemples d'attaques

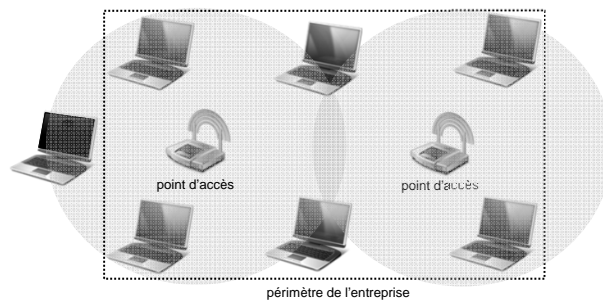


## Attaques sur les réseaux locaux

- Ecoute de réseau (*sniffing*)
  - nécessite un accès physique au réseau
- Redirection de flux
- Usurpation d'adresses (*spoofing*)
  - IP spoofing, ARP spoofing, DNS spoofing, web spoofing ...
- Vol de session (*hijacking*)
- Déni de service par inondation (*flooding*)

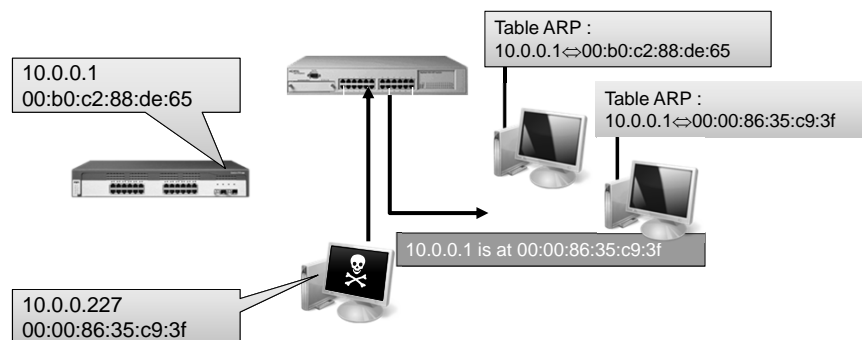
## Wardriving

- Principe : détecter et localiser (éventuellement par GPS) les WLAN dont les ondes radio se propagent à l'extérieur des bâtiments
- Objectifs
  - Utiliser la connexion réseau à son avantage
  - Voler les informations qui transitent sur le réseau



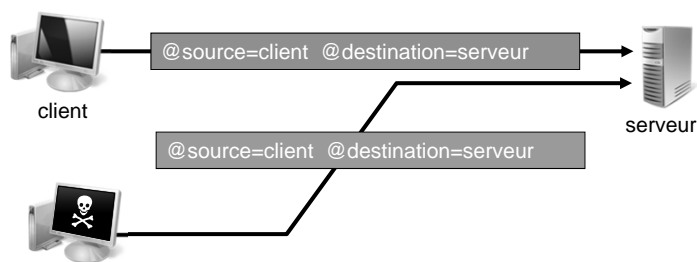
## ARP poisoning

- Principe : corrompre le cache ARP
- Objectif : rediriger le trafic réseau d'une ou plusieurs machines vers la machine du pirate avec des commutateurs (switchs) → capture des trames impossible
- S'effectue sur le réseau physique des victimes



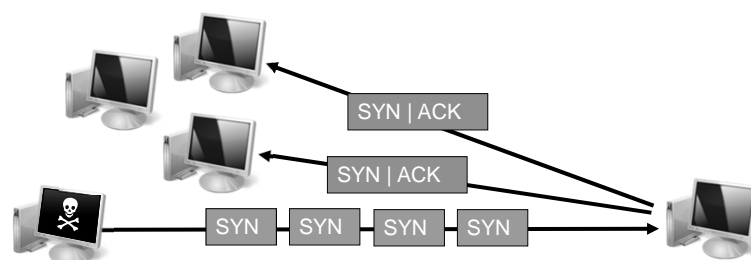
## IP spoofing

- Principe : envoyer un paquet avec une fausse adresse IP source
- Objectifs :
  - Dénis de service
  - Profiter d'une relation de confiance entre deux machines
- Il est impossible de trouver la véritable source du paquet
- L'émetteur ne peut pas recevoir ses réponses



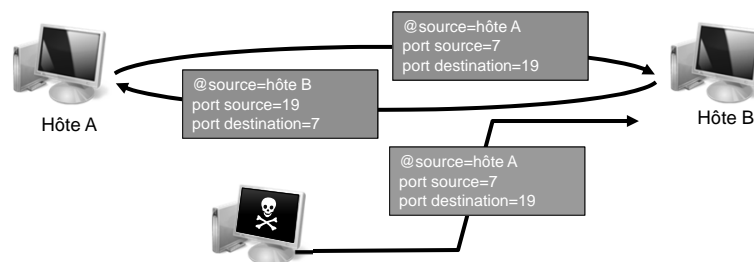
## SYN-flooding

- Principe : envoyer massivement des demandes de connexion (flag SYN à 1) vers la machine cible avec des adresses sources aléatoires
- La machine cible renvoie les SYN-ACK en réponse à chaque SYN reçu
- Aucun ACK n'est renvoyé pour établir la connexion : ces connexions semi-ouvertes consomment des ressources mémoire
- Au bout d'un moment, la machine cible est saturée et ne peut plus accepter de connexions

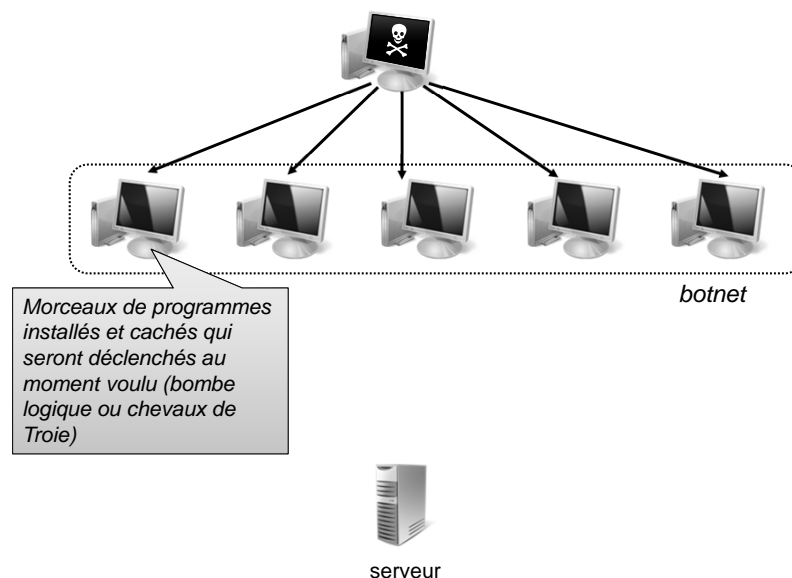


## UDP-flooding

- Principe : générer une grande quantité de paquets UDP (*UDP packet storm*) à destination d'une machine ou entre deux machines
- Utilise le fait qu'UDP (contrairement à TCP) ne possède pas de mécanisme de contrôle de congestion
- Entraîne une congestion du réseau et une saturation des ressources des hôtes victimes
- Exemple le plus connu : *Chargen Denial of Service Attack*
  - faire communiquer le service chargen (génération de caractères, port 19) d'une machine avec le service echo (ré-émission des données reçues, port 7) d'une autre

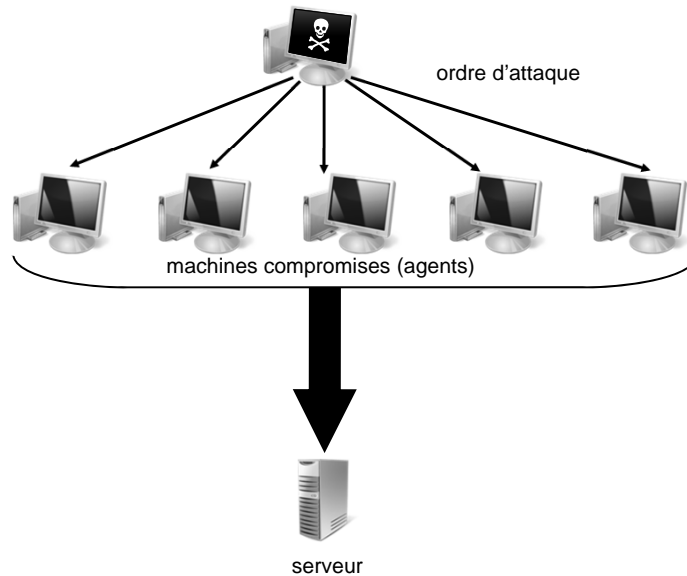


## Les attaques distribuées





## Les attaques distribuées



## Les infections informatiques

- Cheval de Troie (*trojan horse*)
    - programme à priori innocent servant à véhiculer un code destructeur nommé bombe logique
  - Bombe logique
    - programme capable de réaliser une action néfaste de façon différée :
      - consommation boulimique des ressources systèmes (mémoire, CPU, disques ...)
      - destruction de fichiers
      - atteinte à la sécurité du système (mise en place de droits d'accès laxistes, transmission du fichier de mots de passe ...)
      - participation de la machine à des opérations de terrorisme informatique
      - inventaire des numéros de licences des applications présentes sur le disque et transmission chez un éditeur de logiciels
- La sécurité système & réseau – Master IC2A/DCISS – Christian Bulfone

## Les infections informatiques

- Virus
  - morceau de code installé au sein d'un programme hôte, et capable de se répliquer afin d'infester d'autres fichiers exécutables
- Vers
  - programme illicite autonome
- Accès caché (*backdoor*)
  - "trappe" ouverte dans un logiciel souvent non documentée
  - permet à un utilisateur informé d'effectuer une action secrète sur un logiciel, afin d'en obtenir un comportement différent
  - souvent dû au programmeur pour faciliter la phase de débogage de l'application