Introduction à la sécurité

Frédéric Raynal
fred(at)security-labs.org

Cédric Foll
cedric.foll(at)laposte.net

Overview

- Présentation
- Un peu d'histoire
- Introduction à la SSI
- Cryptographie

Première partie I

Présentation

Ma vie, mon œuvre
Fred Raynal

- Diplôme d'ingénieur (spécialité en Intelligence Articifielle)
- Doctorat en Informatique sur le thème de la stéganographie
- Ancien président de SSTIC, conférence francophone sur la sécurité informatique
- Ancien co-responsable du laboratoire SSI d'EADS
- Rédacteur en chef de MISC
- Responsable du laboratoire SSI de Sogeti
- Contributions à des projets open source : scapy, libnet, honeynet

Qui sommes-nous ?
Cédric Foll

- Diplôme d'ingénieur (spécialité en mathématiques)
- Ancien auditeur sécurtié pour la société lexsi
- Ancien RSSI du Rectorat de Rouen (300 sites interconnectés et 20 000 postes de travail)
- Responsable réseau et sécurité du ministère de l'éducation national français (10 000 sites interconnectés et beaucoup trop de postes de travail)
- RSSI de l'année 2006 décerné par 01 réseaux dans la catégorie filtrage web
- Enseignant en second cycle d'ingénieur à l'INSA de Rouen depuis 2005 (réseaux & sécurité) et au ministère de la défense français
- Contribution à des projets libres (prelude, IDS ; Snort, IDS ; DansGuardian, proxy filtrant ; EOLE distribution linux pour les établissements scolaires français)
- Création de logiciels libres (kill-p2p, système anti-peer-to-peer ; pornfind, détection de site pornographiques par filtres bayesiens)

Ma vie, mon œuvre
Innocent Yapi

- École d'ingénieur EPITA (Paris)
- Chef de projets à la CNPS (Caisse Nationale de Prévoyance Sociale)
- S'occupe de la sécurité en général (incendie, électricité et informatique)
- A suivi plusieurs ateliers :
  - 1998 : administration Linux
  - 2002 : infrstructure des réseaux IP
  - 2005 : atelier sécurité

Déroulement de la formation

- Jour 1, AM Introduction, cryptographie et architecture des systèmes
- Jour 1, PM Introduction au réseau
- Jour 2, AM Sécurité Linux
- Jour 2, PM TP système Linux : boot, bind, installation
- Jour 3, AM Sécurité Linux advanced
- Jour 3, PM Forensics + TP
- Jour 4, AM Cours firewall + VPN
- Jour 4, PM TP netkit (+ soirée ?)
- Jour 5, AM Attaques web
- Jour 5, PM TP failles web

Deuxième partie II

Une petite histoire de la SSI

Histoire
Année 1998

Janvier : Root DNS en blackout pour 3 jours

Février : *fairly heavy cyber attacks. . . the most organized and systematic the Pentagon has seen to date.*
Fait par 2 gamins âgés de 15 ans . . .

Mars : des milliers de Win95 et NT plantent
Début de la course aux *nukes*

- Lotus a introduit une *backdoor* dans la version de *Notes* livrée au gouvernement suédois
- 100 attaques par jour contre le Pentagone

Histoire
Année 1999

Janvier : San Diego US Air Force piraté

Mars : les serveurs de l'OTAN *floodés*, sans doute par des serbes

Avril : *Acrobat* installe le cheval de Troie *NetBus*

Septembre : découverte de la chaîne `NSA Key` dans les sources de Windows NT4 SP5

Histoire
Année 2000

- Dénis de service distribué (DDoS) massif contre Yahoo, Amazon, Altavista, . . .
- Ver *I Love You*, première infection virale par e-mail
- Morceaux de code de Win XP volés après une infection virale
- 50 sites web *defacés* par jour

Histoire
Année 2001

Juillet : Ver CodeRed

Octobre : Ver Nimda

- Activité virale en plein essor
- 120 sites web *defacés* par jour

Histoire
Année 2002

- OpenSSH est *trojané*
- 60% des piratages passent par des sites web

Histoire
Année 2003

Janvier : ver SQL Slammer : 90% des machines vulnérables du monde infectées en 10 minutes

Août : Blaster

Août : Sobig, ver qui installe un relai mail pour *spammer*

Septembre : le code source de Valve, le moteur graphique d'Half Life 2, est volé

Octobre : Verisign, détenant les `.com` et `.net`, redirige toutes les requêtes DNS inexistante vers un de leurs sites

Histoire
Année 2004

Mai : ver Sasser, peu d'impact mais très médiatisé

Juin : Akamai hors service pendant 4 jours à cause d'un problème de DNS

Décembre : ver Santy, le 1er à se répliquer en passant par une application web et Google

Histoire
Année 2005

Avril : fichiers sensibles volés à Valeo par une stagiaire chinoise

Septembre : un adolescent est condamné à 11 mois de prison pour avoir piraté le téléphone portable de Paris Hilton

Octobre : Samy, ver XSS infectant MySpace

Décembre : exploit contre Excel en vente sur eBay

- Plus de 100 virus pour mobiles
- Fin des mass mailing virus
- De plus en plus de phishing (ebay, paypal, et toutes les banques partout)
- Le crime paie, plus que le trafic de drogue

Histoire
Année 2006

Novembre : vote d'une loi française reconnaissant le génocide arménien
⇒ des milliers de sites français attaqués par des pirates turcs

Histoire
Année 2007

- Storm botnet
  - Commandé par le réseau P2P Edonkey/Overnet
  - Entre 1 000 000 et 50 000 000 de zombies
  - Utilisé pour DdoS et Spam
- Les principaux pays occidentaux retouvent des trojans chinois dans les réseaux de leurs administrations

En résumé

CodeRed, Nimbda : faille connue avec un patch disponible un an avant la propagation. Toujours actifs aujourd'hui ! ! !

Slammer faille connue, patch disponible depuis longtemps, passe par un port qui n'aurait jamais dû être accessible depuis Internet

Blaster faille connue pour laquelle un patch était disponible depuis 7 jours en passant par un port qui n'aurait jamais dû être accessible depuis Internet

Troisième partie III

Introduction à la SSI

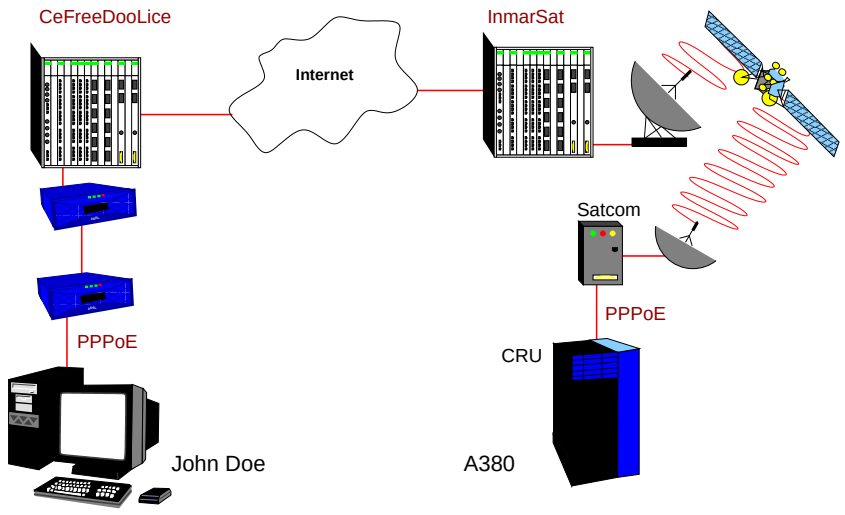
Hein ? Les avions ?

- Beaucoup d'exemples usuels où l'informatique est utilisée
  - Industrie (voiture, pétrole, nucléaire), services (SSII), banques, ...

L'aéronautique

- Les avions n'étaient pas en réseau
- Ils embarquent maintenant des COTS et sont connectés en permanence à Internet

John Doe *vs.* A380



Sûreté *vs.* Sécurité

Sûreté

Un produit est sûr quand il peut fonctionner normalement pour l'environnement dans lequel il est conçu pour fonctionner.

Sécurité

Un produit est sécurisé quand il peut fonctionner normalement pour l'environnement dans lequel il est conçu pour fonctionner.
Cet environnement inclus les gens mal intentionné.

Attaques physiques *vs.* attaques logiques

Attaques physiques

- Un homme avec un lance roquettes peut crasher un avion
- Il doit être proche de l'avion
- L'attaque n'est pas discrète

Attaques logiques

- Un homme qui connaît une faille sur les avions peut crasher *tous* les avions du monde en même temps
- Il peut être n'importe où dans le monde
- L'attaque est certainement très discrète

L'information est partout

Propagation de l'information

- Les ordinateurs se retrouvent partout, partout, partout
- Les Systèmes d'Information (IS) deviennent de plus en plus critiques
- SI sont partout : banques, santé, énergie, transport, défense, ...

Définition (ou pas)

Il est presque impossible de définir ce qu'est un Systèmes d'Information car ça prend beaucoup de formes !

Détermination du périmètre du SI

Éléments informatiques d'un SI

- Ordinateurs portables : connectés au bureau, à la maison, à l'hôtel, à l'aéroport, ..., sans protection particulière
- Mobiles : téléphone portables & PDA deviennent prépondérants, et incorporent de plus en plus de fonctionnalités
- Réseaux : systèmes interconnectant différentes entités ayant chacune des niveaux de sécurité différents

Définition (ou pas)

Un SI n'a pas (plus) une frontière clairement établie, mais *floue*[a]

[a] Ce qui ne veut pas dire qu'il faut pour autant se passer d'un pare-feu !!!

Qu'est ce qu'un système d'information (SI) ?

Définition **réductrice** : système d'information

Un *Système d'Information* est un ensemble d'ordinateurs, connectés de manière permanente ou non les uns aux autres, et permettant à des personnes ou des entités de partager des données (images, documents, programmes, ...) ou de la voix.

Une grande diversité

- Réseau d'opérateurs (telco), mobile ou non
- Sites web d'entités (entreprises, pays, lab, ...)
- Ordinateurs personnels tout comme l'infrastructure du FAI
- Les systèmes militaires *command & control*
- Et de nombreux autres ...

Définition du périmètre du SI

Éléments informatiques d'un SI

- Ordinateurs portables : connectés au bureau, à la maison, à l'hôtel, à l'aéroport, ..., sans protection particulière
- Mobiles : téléphone portables & PDA deviennent prépondérants, et incorporent de plus en plus de fonctionnalités
- Réseaux : systèmes interconnectant différentes entités ayant chacune des niveaux de sécurité différents

Définition (ou pas)

Un SI n'a pas (plus) une frontière clairement établie, mais *floue*[a]

[a] Ce qui ne veut pas dire qu'il faut pour autant se passer d'un pare-feu !!!

Couleurs de l'information

3 couleurs (AFNOR)

- *Information blanche* : information accessible facilement et légalement
  - Ex. : presse, livres, conférences, Internet, ...
- *Information grise* : information accessible légalement mais plus difficile à acquérir
  - Ex. : sources humaines, analyse des dépendances, ...
- *Information noire* : information dont l'accès est restreint et généralement protégé légalement (NDA, CD/SD), seules quelques personnes sont autorisées à y accéder.
  Détenir de telles informations sans y être autorisé conduit à des poursuites judiciaires
  - Ex. : sources humaines, secret du Coca-Cola, Secret Défense, ...

Information encore ...

Criticité de l'information

- Un système d'information est multicolore au regard de l'information qu'il contient
- La capacité à extraire et à analyser de l'information constitue un réel avantage

Dualité de l'information

- Attaquer pour l'information (attaques techniques) : récupérer, altérer, détruire l'information
- Attaquer par l'information (attaques informationnelles) : créer le doute dans l'opinion publique, provoquer la mauvaise conscience chez l'adversaire

Le risque est partout

Risques

L'objectif de la sécurité des SI est de *protéger* les ressources contre les risques liés à l'utilisation d'ordinateurs. Ces risques dépendent de :

- Des *menaces* pensants sur les ressources
- Des *vulnérabilités* des ressources
- De la *sensibilité*, proportionnelle à la valeur donnée aux ressources

Définition (ou pas)

- Équation : risques = menaces * vulnérabilités * sensibilités
- Si un de ces éléments est nul, alors il n'y a pas de risque
- Sécurité = gestion du risque (risk management)

Menaces usuelles

Des menaces partout

- *Utilisateur* : la majorité des problèmes viennent de là (non-implication, malicieux ou simplement maladroit ...)
- *Malware* : logiciels destinés à exploiter un système distant en s'y installant, puis en ouvrant éventuellement ses portes
- *Intrusion* : une personne réussit à accéder à des ressources auxquelles il ne devrait normalement pas pouvoir accéder
- *Sinistre* : mauvaise manipulation ou action malicieuse (incendie, inondation, vol, ...) conduisant à la perte de ressources

Ne pas oublier

- La sécurité information est très technique
- Mais la technique est loin d'être suffisante pour assurer la sécurité

Politique de sécurité

Une première approche

- Ensemble de règles qui décrivent comment l'information doit être manipulée, organisée, gérée.
- Elle repose sur :
  - une analyse de risque
  - un choix de politique
- Elle doit couvrir :
  - tout le système d'information
  - mais aussi son environnement

Définir une politique de sécurité

La construire

- Définir les éléments stratégiques du SI
- Définir le périmètre du SI
- Définir les menaces à anticiper
- Définir les règles à appliquer par tout le monde

Ne pas oublier

Une politique de sécurité doit changer dans le temps, en fonction des nouvelles menaces, frontières, lois, et ainsi de suite.

Cycle de sécurité

Construire la sécurité

- Prévention : démarches préalables destinées à diminuer les risques
  - ex. : charte d'utilisation du SI, sensibilisation, ...
- Détection : mécanismes destinés à prévenir quand un incident se produit
  - ex. : anti-virus, cellule de veille
- Restauration : remise en état quand tout le reste à échouer
  - ex. : *forensics*, PRA (Plan de reprise d'activité)

Champ de bataille : du côté de l'armée

Une question d'échelle

- *Niveau stratégique* : les généraux et les politiciens, leur objectif est de remporter la guerre, ils ne se préoccupent pas de batailles spécifiques
- *Niveau tactique* : les colonels et commandants qui cherchent à gagner leurs batailles, ils ne se préoccupent pas des combats sur le champ de bataille
- *Niveau opérationnel* : les sergents et soldats, ils suivent les ordres et essayent de survivre sur le champ de bataille

À appliquer en SSI

Appliquer le même découpage à la sécurité des SI (politiques, architectures, implémantions)

Objectifs de la sécurité

Cible de sécurité

- *Confidentialité* : assurer que seules les personnes autorisées ont accès à une ressource donnée
- *Intégrité* : assurer qu'une ressource n'a pas été altérée, est reste donc pertinente
- *Disponibilité* : assurer qu'une ressources est accessible quand on en a besoin
- *Authentification* : assurer qu'une personne est bien qui elle prétend être
- *Répudiation* (US only) : assurer qu'une personne ne peut pas nier avoir accompli une action quand elle l'a fait

Ne pas oublier

- La sécurité pour la sécurité ne sert à rien
- La sécurité ne sert qu'à protéger des ressources

Qu'est ce que la *Sécurité des systèmes d'information* ?

Cherche à garantir que les systèmes d'information fonctionnent :

- Confidentialité
- Intégrité
- Disponibilité
- Non-répudiation
- Authentification

Confidentialité

Protéger l'accès aux ressources :

- par les utilisateurs
- par les applications (lancées par les utilisateurs)
- par le système (qui exécute les applications lancées par l'utilisateur)

$\Longrightarrow$ politique pour accéder à l'information

Outils

- Authentification
- Contrôle d'accès
- Chiffrement (symétrique essentiellement)

Intégrité

Garantir la consistance d'un système d'information :

- Les données ne sont pas altérées ou détruites, volontairement ou non
- Nécessite une connaissance approfondie des mécanismes du système

Outils

- Contrôle d'accès
- Code correcteurs
- Cryptographie (hash, signature numérique)

Disponibilité

Garantir que des utilisateurs légitimes pourront accéder aux ressources dont ils ont besoin

Outils

- Contrôle d'accès
- Tolérance aux fautes
- Équilibrage de charge

Vers de nouveaux modèles

Évolutions

- Le *hacker* n'est plus (ou plus seulement) un jeune adolescent qui mange de la pizza et boit du Coca (light)
- Les attaques dangereuses sont invisibles, ne reposent pas (uniquement) sur des exploits techniques, et sont difficiles à repérer
- L'insécurité devient un vrai business
  - des botnets ou des routers BGP sont vendus (et achetés !) sur eBay
  - Une entreprise israélienne loue son cheval de Troie : des dirigeants partout autour du monde ont été arrêtés
  - Une *major* vend des CDs avec un root-kit : ça envoie des données à la major, ça ouvre une faille dans la machine, ça contient du code volé

Objectifs techniques d'une attaque informatique

Une question de tactique

- Empêcher l'accès à une ressource sur le système (*Denial-of-Service, DoS*)
- Prendre le contrôle du système, par exemple, pour l'utiliser dans une phase ultérieure (un (d)DoS)
- Récupérer de l'information stockée sur le système (ex. des spywares ou chevaux de Troie)
- Utiliser le système pour rebondir, et propager plus avant son attaque

Do not forget

Ces choix sont indépendants des compétences de l'attaquant, du script kiddie aux services d'État.
De plus, ces opérations font souvent partie d'une stratégie plus globale.

Pourquoi ces attaques informatiques ?

Exemples des motivations les plus classiques

- *Fun* : souvent pour se vanter auprès de ses amis
  - Ex. de moyens : utilisation d'exploits prêts à l'emploi, faible niveau de compréhension
- *Argent* : pour retirer un bénéfice pécunier
  - Ex. de moyens : vente de machines compromises
- *Message idéologique* : faire passer un message à caractère religieux, politique, éthique ...
  - Ex. de moyens : *defacement* de sites web à forte audience
- *Information* (donc l'argent) : pour obtenir une information qui sera utile ensuite (soit une commande, soit du chantage, soit de l'espionnage industriel, ...)
  - Ex. de moyens : *trojan horses* construits sur mesure

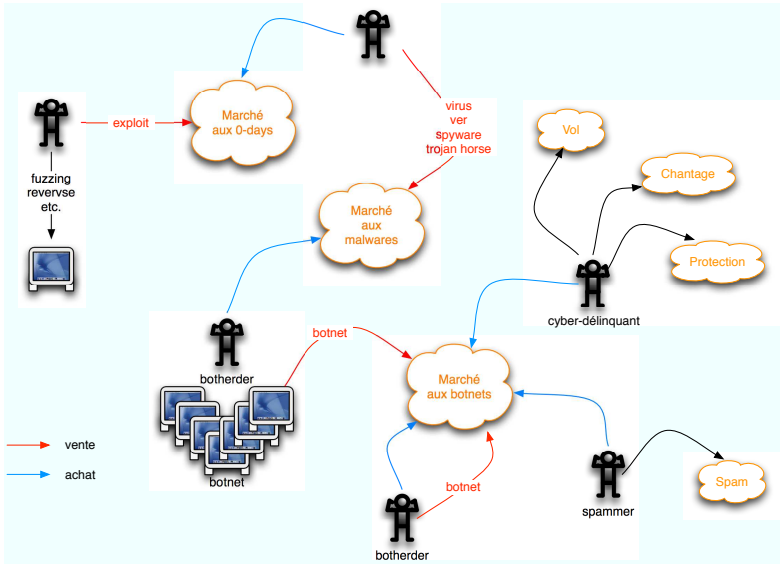
Le fun

Un groupe de w4rl0rDz

Un groupe de pirates roumains dont le site web a 3 entrées :

- `forum.w4rl0rDz.org` : vente/échange d'exploits
- `fucking.w4rl0rDz.org` : site principal de la t34m
- `exploits.w4rl0rDz.org` : site secret . . . sans aucune protection

L'argent



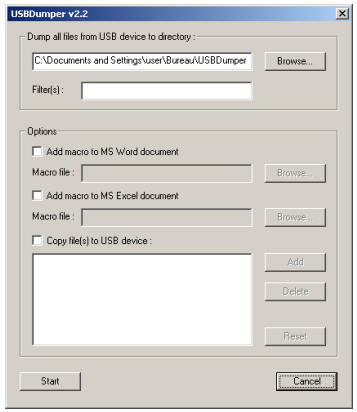
L'idéologie

Le cyber-moudjahidine

- L'art de la dissimulation de fichiers
- La géolocalisation par satellite
- Comment protéger les *communiqués* en cas d'intrusion
- Introduction à PGP : est-il assez sûr pour les cyber-moudjahidines ?

La première mission du djihad informatique est de combattre et vaincre moralement l'ennemi. Le djihad informatique permet d'avoir des impacts plus destructeurs que les armes de guerres classiques.

L'information



USBDumper

- On branche sa clé USB sur un ordinateur inconnu
- Tout ce qui est dessus est recopié sur le disque dur
- On ajoute des macros aux documents MS Office
- Variante : on clone la clé pour analyser les fichiers effacés plus tard

Où attaquer un SI ?

Attaquer partout :)

- *Éléments physiques* : attaquer les infrastructures (ex. : vol ou destruction), ordinateurs ou même les câbles
- *Électronique* : intercepter ou brouiller les communications
- *Software* : utiliser des logiciels pour rentrer dans des SI, les explorer, en prendre le contrôle ou les détuire
- *Humain* : toujours le maillon faible, que ce soit par corruption, manipulation, intoxication, ...
- *Organisation* : envoyer un stagiaire, ou un faux candidat pour répondre à un annonce qui agit ensuite comme un cheval de Troie

Ne pas oublier

Définir sa politique de sécurité sans prendre en considération tous ces risques est aussi utile que fermer une porte tout en laissant les fenêtres ouvertes

Comment organiser sa sécurité ?

4 composants

- Juridique : chiant *a priori* car impose un cadre pas toujours pertinent, ne sert qu'*a posteriori* quand il est trop tard
- Organisationnel : chiant tout le temps car impose un ensemble de normes aux entités que les personnes prennent un malin plaisir à ne pas respecter
- Technique : chiant pour tout le monde sauf les *geeks*, et comme personne ne parlent leur langage, ils ne parlent qu'entre eux
- Humain : aussi appelé *le maillon faible*, source d'émerveillement quotidien

Le terrain de jeu (1/2)

Sécurité de l'information

La sécurité de l'information s'intéresse à tous les "domaines" susceptibles de contenir de l'information, de la faire transiter, de la manipuler[a], bref, aux *vecteurs*.

[a] Au sens de la modifier, et non au sens intoxication et autres, bande de pervers

Le terrain de jeu (2/2)

***In*Sécurité de l'information**

L'*in*sécurité de l'information s'intéresse à tous les "domaines" susceptibles de contenir de l'information, de la faire transiter, de la manipuler[a], bref, aux *vecteurs*.

[a] Au sens de la modifier, et non au sens intoxication et autres, bande de pervers

Comment organiser l'*in*sécurité ?

4 composants

- Juridique : épuiser les ressources de l'adversaire, le pousser à dévoiler des informations, ...
- Organisationnel : saturer les fournisseurs, débaucher les prestataires, passer par les filiales, accéder aux services externalisés ...
- Technique : exploitation des failles dans les logiciels, *backdoors* et autres *spywares*, ...
- Humain : mots de passe faibles, MICE (Money, Ideology, Coercion, and Ego), ...

Et si les attaques ciblées n'étaient pas si compliquée ?

Bêtises et/ou faiblesses humaine

- Exploiter des failles techniques s'avère souvent compliqué
- Profiter des erreurs d'autrui est souvent beaucoup plus facile
- Rien n'est impossible, même l'incroyable ...

Attaque ciblée depuis l'extérieur

Phases de l'attaque

- Environnement : recherche de toutes les informations pertinentes sur la cible (DNS, adresses mail, téléphone, annuaires, identification des services/applications réseau ...)
- Recherche des failles[a] : analyse des informations obtenues pour pointer les failles, et trouver les méthodes d'exploitation
- Planification : mise en place d'un plan d'action, d'un plan de secours, tests des outils, avant de lancer l'assaut
- Exploitation : utilisation des angles d'attaque retenus et pérennisation, si besoin, de l'accès obtenu

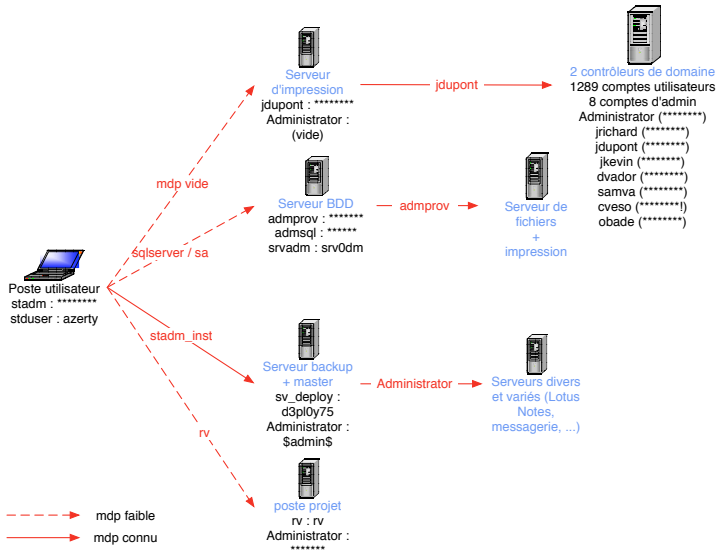
[a] Pas uniquement des failles techniques !

Attaque ciblée depuis l'intérieur

Phases de l'attaque

- Augmentation locale de privilèges :
  - Passer Administrateur sur son propre poste si on ne l'est pas
  - Récupérer les mots de passe locaux et du cache ... puis les casser
- Explorer le réseau : identifier les éléments importants du réseau (contrôleurs de domaine, serveurs de fichiers, back-ups, ...)
- Identifier les admin : identifier les multiples comptes d'administration du domaine
- Rechercher les erreurs humaines : les mots de passe faibles sur les serveurs importants, les anciens serveurs migrés depuis, ...
- Rebondir sur un nouveau serveur, récupérer puis casser les mots de passe locaux et du cache

Attaque ciblée depuis l'intérieur par la pratique



Une histoire de mots de passe

Statistiques sur 1289 mots de passe d'une base SAM

- 7 mdp == login
- 46 (3.6%) login contenu dans le mdp
- 111 (8.6%) mdp contiennent le nom de l'entité ou d'une filiale
- 36 (2.6%) ne contiennent que des chiffres, dont 27 sont 12345678, le mdp par défaut (donc jamais changé)

Temps de cassage

- Par brute-force, plus de **1000 mdp sur 1289 sont tombés en 3h**
  - Utilisation d'un laptop standard pour ça !
- En utilisant les *rainbow tables*, en moins d'une nuit, il reste moins de 10 mdp à casser (dont 4 de plus de 14 caractères, donc incassables[a])

Durée totale pour la prise de contrôle complète du réseau : une semaine

[a] Avec les outils / techniques actuels !

Quatrième partie IV

Introduction à la cryptographie

Outline

Qu'est ce que la cryptographie ?

Objectif

- La cryptographie est la science du *secret*
- Elle cherche à définir des algorithmes (schémas, protocoles) qui garantissent une propriété donnée, même dans un environnement hostile

De la crypto partout

- Téléphones portables
- Cartes de crédit
- Protections logicielles
- Transactions bancaires
- Internet
- ...

À quoi ça sert ?

Problèmes de sécurité

La crypto doit fournir des solutions aux problèmes évidents de sécurité

Exemples de fonctionnalités

- Assurer le secret des informations (ou comment les lettres d'amour ne doivent être lisibles que par leur destinataire)
- Identifier une source d'information
- Autoriser une action (ou en interdire, comme la copie de logiciel)
- Donner les accès à des ressources (entrer dans une pièce, accéder à un fichier)
- Vérifier l'intégrité des informations
- Fournir un document signé
- ...

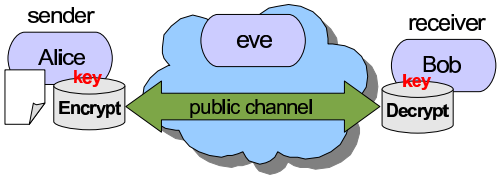
Opérations élémentaires

Opérations cryptographiques

- Chiffrement/déchiffrement : protocole destiné à garantir le secret d'un *texte clair* en produisant un *texte chiffré* (chiffrement) qui ne peut être retransformé vers sa forme initiale (déchiffrement) que si une information secrète (la clé) est connue
- Signature numérique : protocole destiné à assurer l'authentification et l'intégrité d'un document (non répudiation)
- Empreinte (Digest, Hash) : algorithme destiné à fournir un mécanisme de vérification de l'intégrité, principalement employé comme brique dans d'autres protocoles
- Générateurs pseudo-aléatoires : algorithmes destinés à se comporter comme une vraie source d'aléa

Schéma et conception

Alice, Bob et Eve

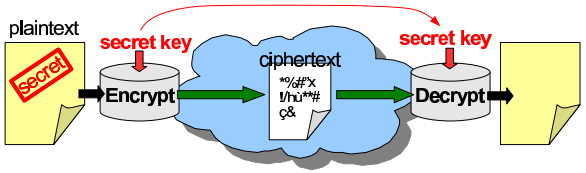


Principe général : algorithme et clé

Un protocole cryptographique est un algorithme qui prend une *information* et une *clé* pour produire un résultat dépendant de ces 2 entrées.
La sécurité du protocole ne doit dépendre que de la clé, et non sur la méconnaissance de l'algorithme qui, lui, devrait être public (ex. : les protocoles GSM, CSS, SDMI ont été cassés bien que secrets).

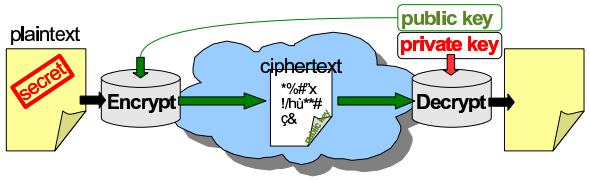
Chiffrement symétrique

- Une seule clé secrète, seulement partagée par Alice et Bob



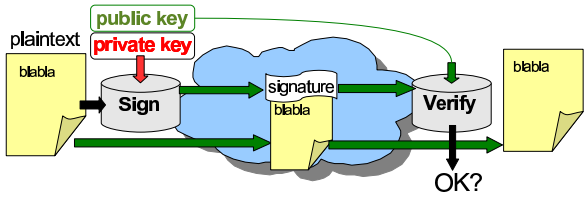
  - Objectif : le secret de l'information
  - Problème : comment partager la clé secrète ?

Chiffrement asymétrique



- Bi-clés de Bob : une clé privée, seulement connue de Bob, et une clé publique
- Alice chiffre le message avec la clé publique de Bob
- Seul Bob peut déchiffrer à l'aide de sa clé privée

Signature numérique

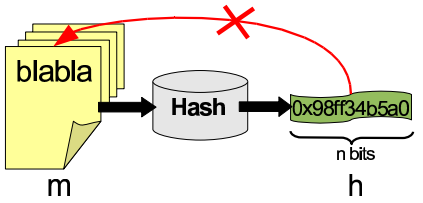


- Alice dispose de sa propre paire de clés
- Elle peut signer un message avec sa clé privée
- Bob authentifie le message avec la clé publique d'Alice

Primitives : fonctions de hash

Fonctions one-way (à sens unique)

Une fonction $H : m \in \{0,1\}^* \rightarrow h = H(m) \in \{0,1\}^n$ vérifie la propriété que, étant donné h, il est *très difficile* de retrouver une pre-image m.

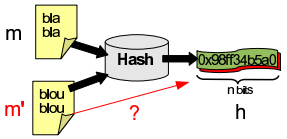


La valeur h est appelée *empreinte* ou *hash* du message m

Primitives : fonctions de hash

Problème des collisions

- Le nombre de messages possible est infini
- Mais il y a un nombre fini de hash ...
- Problème : peut-on facilement trouver des collisions ?

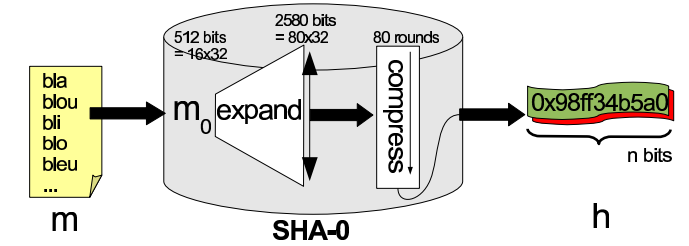


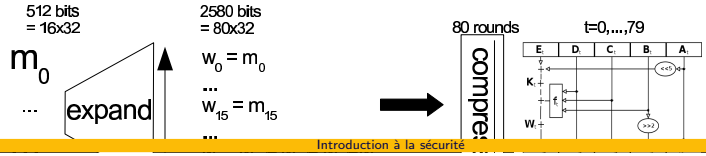
- Pre-image : soit h, trouver m
- Collisions : trouver m et m' pour un même h
- 2ème pre-image : soit m et $h = H(m)$, trouver m' avec $H(m') = h$

Primitives : fonctions de hash

Les fonctions SHA

- Le message m est coupé en blocs de 512 bits
- Chaque bloc est étendu en un bloc intermédiaire de 2560 bits
- Ce bloc intermédiaire est compressé en bloc de 160 bits





Primitives : fonctions de hash

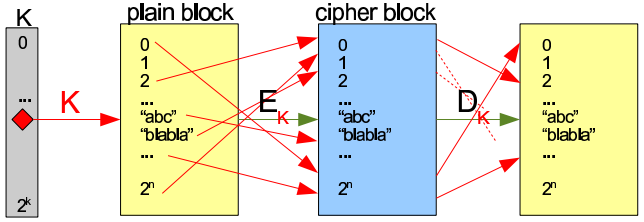
Autres exemples

- MD5 ($n = 128$) : cassée, remplacement nécessaire
- SHA-0 ($n = 160$) : cassée mais inutilisée
- SHA-1 ($n = 160$) : cassée, remplacée après 2010
- SHA-2 (SHA256 $n = 256$, etc) : **sûre** mais construite sur des bases faibles ?

Primitives : chiffrement par blocs

Permutations aléatoires

- Un chiffrement par blocs est une famille de permutations $(E_K)_{K \in \{0,1\}^k}$
- Pour une clé K, le chiffrement est une permutation de l'ensemble $\{0,1\}^n$
- Propriété : ne peut pas être distinguée d'une famille aléatoire de permutations

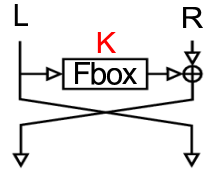


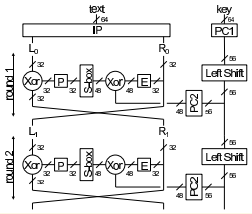
Sécurité : résistance à la cryptanalyse linéaire et différencielle

Primitives : chiffrement par blocs

Exemple : DES

- Un réseau de Feistel : blocs de 64 bits = 2x32 bits
- Une clé de 56 bits produisant 16 sous-clés
- 16 rounds





Primitives : chiffrement par blocs

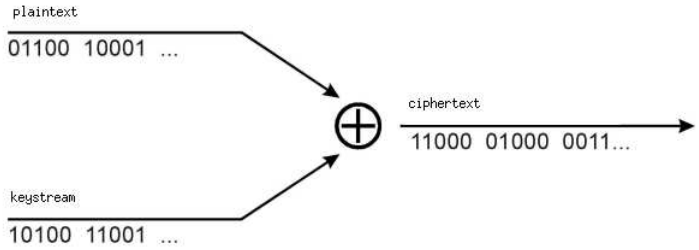
D'autres exemples

- DES ($n = 64$) : cassé par cryptanalyse linéraire et maintenant menacé par le brute-force (clé de seulement 56 bits)
- 3DES ($n = 64$) : sûr (clé de 112 bits) mais 3 fois plus lent que DES ! ! !
- AES ($n = 128$) : sûr (clé de 128, 192 oou 256 bits), bonnes performances. . .

Primitives : chiffrement par flot

One-Time pad et suite pseudo-aléatoire

- One-Time Pad (chiffrement de Vernam, $c_i = m_i \oplus k_i$) est inconditionnellement sûr pour une suite aléatoire servant de clé
- Un générateur pseudo-aléatoire est une fonction $G : K \in \{0,1\}^k \rightarrow \{0,1\}^*$ telle que la sortie ne peut pas être distinguée d'une suite aléatoire



Sécurité : dépend de l'aléa de la suite clé

Primitives : chiffrement par flot

Exemple : RC4

- L'initialisation de RC4 (appelée KSA) utilise une clé de 128/256 bits
- Une suite pseudo-aléatoire est alors générée (PRGA)

RC4 PRGA (pseudorandom generation algorithm)

état initial : $S^0 = S_{255}$, $i = 1$ et $j_0 = 0$, sortie : $(o_i)_{i \in \mathbb{N}}$:

$$j_i = j_{i-1} + S^{i-1}(i)$$
$$S^i(i) \rightleftharpoons S^i(j_i)$$
$$o_i = S^i(S^i(i) + S^i(j_i))$$

Primitives : chiffrement par flot

Autres exemples

- A5/1 ($k = 64$) : cassé, utilisé dans le standard GSM
- FISH (Siemens, 93) : cassé dès qu'on connaît environ 1000 textes clairs
- Pike (1994) : FISH amélioré
- Phelix (2004, eSTREAM contest) : très rapide, avec authentification

Primitives : RSA

Factorisation / Racine n-ième

Choisir des nombres premiers p, q. On note $n = pq$, la paire de clés est alors :

- Clé privée : (d, n)
- Clé publique : (e, n) avec $e.d = 1 \mod \phi(n)$ (besoin de connaître p, q)

Pour chiffrer un message m, on calcule

$$c = m^e \mod n$$

Pour déchiffrer, on a besoin de la clé privée :

$$c^d \mod n = (m^e)^d \mod n = m$$

Sécurité : factoriser de grands entiers est difficile.
Calculer la racine n-ième est difficile (RSA Problem)

Primitives : El Gamal

Log Discret

Choisir n, g un nombre premier et un générateur du groupe $\mathbb{Z}_n^*$, la paire de clés est :

- Clé privée : a
- Clé publique : y avec $y = g^a \mod n$

Pour chiffrer un message m, choisir un nombre aléatoire k

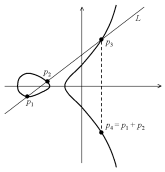
$$c_1 = g^k \mod n$$
$$c_2 = y^k.m \mod n,$$

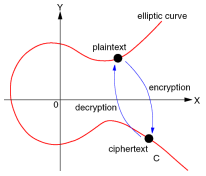
Pour déchiffrer, on a besoin de la clé privée :

$$c_1^{-a} c_2 \mod n = g^{-ak}(g^a)^k.m \mod n = m$$

Sécurité : le log discret est un problème difficile (DL Problem)

Primitives : courbes elliptiques





Log discret dans un groupe cyclique "généralisé"

Une courbe elliptique est définie par une équation de la forme $y^2 = x^3 + ax + b$.
Les paramètres publiques sont un point P d'ordre premier n sur la courbe.

- Clé privée : d
- Clé publique : $Q = dP$
- El Gamal devient $C_1 = kP, C_2 = M + kQ$ et $M = C_2 - dC_1$.

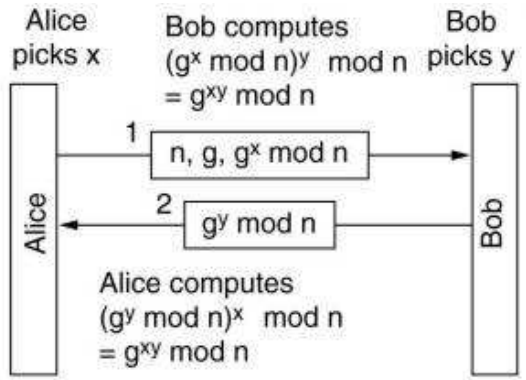
Avantages et inconvénients

- Efficacité : comparaison des tailles de clé pour un niveau de sécurité équivalent

	3DES (112)	AES (128)	AES (192)	AES (256)
EC	224	256	384	512
RSA	2048	3072	8192	15360

- Performances : bonnes en symétrique, mauvaises en asymétrique
- Sécurité : bases mathématiques pour l'asymétrique
- Gestion des clés : bien pour l' asymétrique (pas de clé à partager), mauvais en symétrique
- Chiffrement : par flot est très rapide mais demande de la synchronisation, par blocs sont robustes et étudiés depuis longtemps

Diffie-Hellman, où l'échange de clés tranquille



Diffie-Hellman

Utilisation d'un système à clé publique pour échanger une clé secrète (pour du chiffrement symétrique) au travers d'un canal non-sécurisé (PKCS#3)