Cryptologie et Sécurité Informatique

Tidiane Diallo

January 4, 2023

Introduction

Cryptologie et sécurité informatique

Deux points de vue

1. cryptologie, application à la sécurité informatique et réseaux
2. sécurité informatique et réseaux, utilisation de la cryptologie

Evaluation

1. contrôle continu : TPs
2. Examens

Plan général

1. Introduction à la sécurité et à la cryptologie
2. Cryptologie
3. Sécurité informatique et réseau

Sommaire

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 systemes et systèmes et ressources informatiques.
- Notamment, on veut préserver
  - l'intégrité de l'information
  - la confidentialité de l'information
  - la confidentialité de l'information
- Systèmes informatiques soumis à des menaces
  - utilisateur du système
  - personne malveillante
  - programme malveillant

Cryptographie et cryptanalyse

Définition (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.

Définition (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

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
authenticafition : vérification de l'identité de l'utilisateur et de ses autorisations
non-répudiation : imputabilité, traçabilité, auditabilité

Domaines d'intervention de la sécurité

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, authentiication)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, dimensionnement)
- alentours (pare-feu, vpn, nomadisme)

Menaces informatiques

sécurité physique
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 préjudiciables

- en permanence sur Internet par machines infectées
- rarement pirates

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)

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
- Typologie : malveillance, erreur, accident
- Cibles : états, organisations, individus
- Vol d'identité, Chantage, Fraude financière, détournements de fonds, vol de biens virtuels, atteinte à la dignité, dénonciation calomnieuses, espionnage, cyberterrorisme, désinformation, apologies de crimes, escroqueries, atteinte aux mineurs, atteinte à la vie privée, incitation à la haine raciale, ...

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 $\Longrightarrow$ ubiquité, anonymat
- immatérialité : information numérique peut être détruite, modifiée, usurpée
- disponibilité d'outils, paradis numériques
- dépendance des états/organisations à l'informatique $\Longrightarrow$ facteur de risque $\Longrightarrow$ cyberterrorism

Typologie des attaques

- accès physique : coupure électricité, vol de disque dur, écoute traffic réseau, récupération de matériels
- interception de communications : vol de session, usurpation 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, débordements de tampon
- trappes : porte dérobée dans un logiciel
- ingénierie sociale : contact direct de l'utilisateur
- attention aux attaques par rebond : l'utilisateur "complice" peut voir sa responsabilité engagée.

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)
- **backdoor (ou Porte dérobée)**: Fonctionnalité inconnue de l'utilisateur, qui donne un accès secret au logiciel/système Trusting Trust (1984), noyau Linux (2003).

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
- **polupostage ou spam** (98 % des mails)
- **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 (disquette, disque)

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 d'éradication 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

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.