Sécurité des systèmes et des réseaux

Emmanuel CONCHON
(emmanuel.conchon@univ-jfc.fr)

Bibliographie

- « Cryptographie et sécurité des systèmes et des réseaux », Touradj Abrahimi, Franck Leprévost, Bertrand Warusfel, 2006
- « Cryptography and Network Security Principles and Practice, 5th Edition », William Stallings
  - Des figures du cours sont tirées de cet ouvrage
- « Les réseaux », Andrew Tanenbaum
  - Chapitre 8
- « Les systèmes d'exploitation », Andrew Tanenbaum
  - Chapitre 9

Plan du cours

- Introduction générale à la sécurité informatique
  - Définitions et objectifs
  - Mécanismes d'intrusions/d'attaques
  - Les services de sécurité
  - Mécanismes de défense
- La cryptologie
  - Chiffrement symétrique
  - Chiffrement asymétrique
  - La signature électronique
- Sécurité des réseaux
  - Sécurité des mails
  - Firewall et architectures de sécurité
  - Transport Level Security (TLS)

Introduction générale

« Connais ton ennemi et **connais-toi toi-même**; eussiez vous cent guerres à soutenir, cent fois vous serez victorieux.
Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales.
Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites. »

Sun Tzu « L'Art de la Guerre »

« Se faire battre est excusable, se faire surprendre est impardonnable ! »

Napoléon

Introduction générale – Définition et objectif

- Définition Wikipédia
  - La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques
  - Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information
- L'objectif est de minimiser la vulnérabilité d'un système informatique
  - Un système informatique connecté ne peut pas être complètement sûr!
- Elle permet de se protéger contre des menaces intentionnelles ou des menaces accidentelles

Introduction générale – Définitions et vocabulaire

- Vulnérabilité
  - Faiblesse ou faille introduite de manière intentionnelle ou accidentelle durant la spécification, la conception, le développement ou le déploiement d'un système (matériel ou logiciel)
- Attaque
  - Action malveillante visant à exploiter une vulnérabilité d'un système et qui viole un ou plusieurs besoins en sécurité
- Intrusion
  - Faute externe résultant de l'exploitation réussie d'une vulnérabilité
- Menace
  - Violation potentielle d'une propriété de sécurité
- Risque
  - Menace + vulnérabilité

Introduction générale – Définitions et vocabulaire

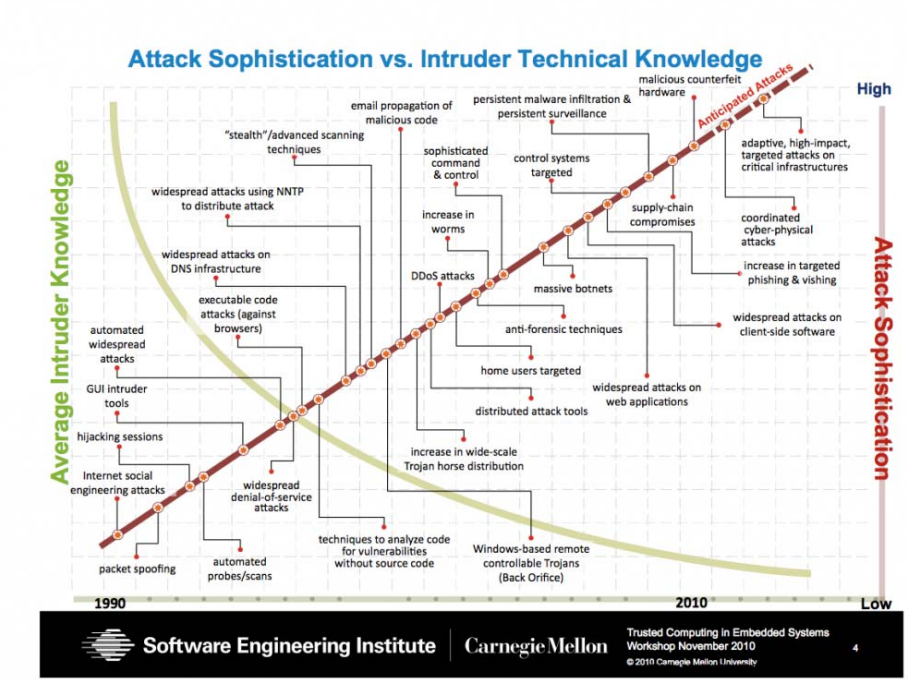
- Virus
  - Bout de programme qui lorsqu'il s'exécute s'auto réplique et se greffe sur un autre programme pour en modifier le comportement
    - Peut évoluer en cheval de Troie
- Vers
  - Comme le virus, le ver est un programme malveillant qui se diffuse à travers le réseau, mais à la différence du virus, il fonctionne de manière autonome et ne se réplique pas sur la machine
- Spyware
  - Logiciel qui s'installe dans le but de collecter et de transmettre des données sur le réseau à l'insu de l'utilisateur du système compromis
    - Ex: Keylogger

Introduction générale – Définitions et vocabulaire

- Bombe logique
  - Bout de programme qui reste en sommeil jusqu'à ce que des conditions particulières surviennent pour causer des dommages
    - Les virus, chevaux de Troie et vers contiennent des bombes logiques
- Porte dérobée
  - Fonctionnalité permettant de contourner un mécanisme de sécurité à l'insu de l'utilisateur
  - Il peut s'agir soit d'une vulnérabilité du système qui peut être intentionnelle ou accidentelle
    - Elles peuvent par exemple être aménagée à l'origine dans un but de test et de maintenance
- Cheval de Troie
  - Programme effectuant des actions néfastes sous l'apparence d'un programme autorisé

Introduction générale – Définitions et vocabulaire

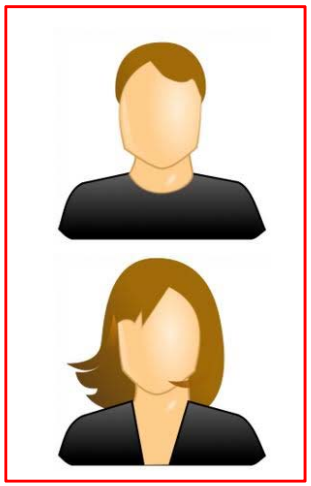
- Spam
  - Message non sollicité obtenu par une utilisation abusive d'une boite mail
    - Le premier spam date de 1978 et a été envoyé par Gary Thuek à destination de tous les utilisateurs d'ARPANET (600 personnes)
- Sniffing
  - Accès illégales à des données sur un canal de communication ou sur un support vulnérable pour obtenir des informations sensibles
- Spoofing
  - Usurpation d'identité pour obtenir des informations ou des accès
- Déni de service (DDS et dDDS)
  - Attaque d'un serveur ayant pour but de l'empêcher de rendre son service
    - En général on surcharge le serveur de requêtes
  - Le dDDS est un déni de service distribué s'appuyant sur plusieurs centaines de terminaux zombis pour générer les requêtes



Introduction générale – Les sources de risque

Danger élevé mais risque d'occurrence faible

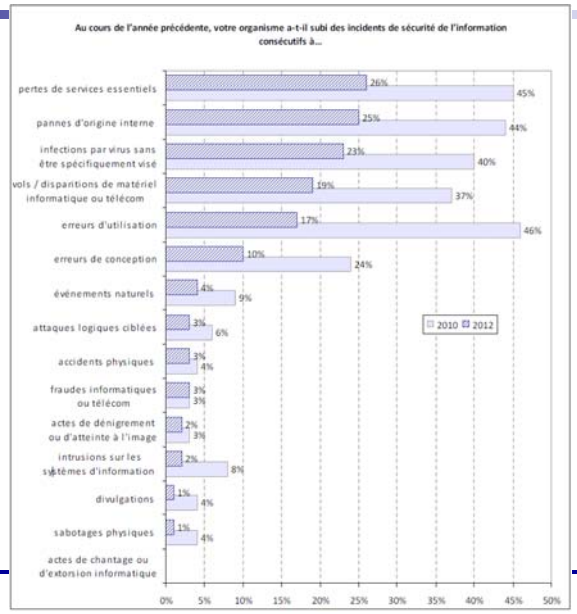
V.S



Danger modéré mais risque d'occurrence très fort

Introduction générale – Les sources de risque

Source: CLUSIF pour l'année 2011



Introduction générale - CID

- La sécurité informatique repose sur trois piliers (triade CID)
  - La confidentialité
    - Des données informatiques
    - Des données à caractère personnel
  - L'intégrité
    - Des données
    - Des systèmes
  - La disponibilité

- On peut également leur adjoindre
  - Authenticité/Authentification
  - Traçabilité (Accounting en anglais)
    - Inclue la non-répudiation des données

Introduction générale - Confidentialité

- La confidentialité consiste à garder secret le contenu d'une information
  - Il faut empêcher sa lecture et sa divulgation à toute entité non autorisée
- Il faut donc mettre en place des mécanismes pour rendre cette information inintelligible par des tiers non autorisés
  - Lors de la conservation
  - Lors de la sauvegarde
  - Lors du transfert
- La confidentialité recouvre aussi la nécessité de laisser à un usager le contrôle sur ses informations personnelles
  - Accès, modification, masquage, suppression

Introduction générale - Intégrité

- L'intégrité des données doit être assurée par tous les moyens contre
  - Les modifications accidentelles
  - Les modifications volontaires
- L'objectif est d'assurer que des informations sauvegardées ou transmises sont bien conformes aux données d'origine
- Nécessite la mise en place de contrôle d'accès pour la modification des données
  - Seules ont le droit de modifier les données, les personnes explicitment autorisées à le faire

Introduction générale - Disponibilité

- Les données doivent être accessibles de manière fiable par toutes les entités autorisées
- La disponibilité consiste à mettre en œuvre les moyens matériels nécessaires pour assurer
  - La bonne conservation des données
  - Le bon fonctionnement du système
- Concrètement cela peut consister à mettre en œuvre un système de redondance des services pour palier à l'indisponibilité d'un service particulier
  - Ex: Les Content Delivery Network

Introduction générale - Authenticité

- L'objectif est d'assurer qu'une entité est bien ce qu'elle prétend être
  - Pour garantir la qualité de l'information qu'elle fournie
  - Pour s'assurer qu'elle a le droit d'effectuer certaines actions
- Dans le cas d'une transmission l'authenticité devra assurer que l'information reçue est bien celle qui avait été envoyée
- L'authenticité d'une personne (ou identification) va permettre de limiter les accès aux seules ressources nécessaires
  - La preuve de l'identité donne des droits qui ne permettent normalement pas un accès total à toute l'information
- L'authentification permet de vérifier
  - L'origine d'une information
  - L'identité d'une personne

Introduction générale - Traçabilité

- Chaque action sur l'information doit pouvoir être tracée de manière à permettre de détecter une faille à posteriori
- La traçabilité est indispensable pour disposer de preuves lors d'une intrusion ou pour prouver la modification de données
- Permet d'assurer la non répudiation de certaines actions qui ont pu être effectuées sur le système
  - Une personne ne doit pas pouvoir nier avoir reçu une information par exemple

Introduction générale – Démarche à avoir

- Démarche générale
  - Identification et évaluation des risques
  - Etablissement d'une politique de sécurité
  - Mise en place de la solution de sécurité, des contre mesures
    - Inclue la formation et la sensibilisation des usagers
  - Auditer/évaluer la solution mise en place
- Cette démarche doit être répétée périodiquement!
  - En particulier la phase d'audit
  - Une solution de sécurité n'a qu'une durée de vie limitée et doit être réactualisée
    - Virus
    - Failles dans les logiciels
    - Utilisateurs
    - …

Introduction générale – Quelques procédures

- Définition du domaine à protéger
  - Tout n'est pas critique, il ne faut protéger que le nécessaire
- Définition de l'architecture de sécurité
  - Equipements
  - Paramètres de sécurité et mécanismes de prévention et de détection
- Prévoir les failles
  - plan de continuité d'activité et plan de reprise d'activité
- Elaboration de chartes à destination des utilisateurs
  - Sensibilisation aux risques, faire adhérer à la politique globale
- Gérer l'évolution des RH (départ, arrivé de nouveaux éléments) et du système
  - Définition d'un organigramme précis avec les responsabilité de chacun
- Définition de méthodes de développement sûres, de mise à jours des failles
- …

Introduction générale – Le facteur humain

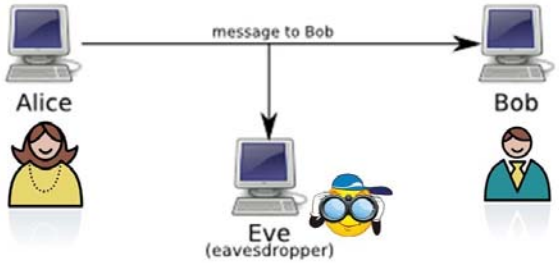
- Le facteur humain demeure toujours l'élément le plus important d'une politique de sécurité
  - La plupart des vulnérabilités viennent des utilisateurs
    - non respect des procédures
    - incompréhension de l'intérêt d'une procédure
    - surcharge induite par des procédures sur l'activité
  - Un système n'est fiable que si tout le monde joue le jeu
    - On ne donne pas son mot de passe à un collègue
    - On ne le laisse pas sur un post-it
    - …

L'architecture de sécurité OSI

- Définit par l'ITU-T dans sa recommandation X.800
- Son objectif est de fournir une approche systématique pour évaluer et choisir des moyens de sécurité adaptés à des communications distribuées
- Elle s'intéresse à trois aspects de la sécurité réseau
  - Les attaques
    - Passives
    - Actives
  - Les mécanismes de sécurité
    - Détection
    - Prévention
    - récupération
  - Les services de sécurité
    - Amélioration de la sécurité
    - Mise en échec des attaques

Les attaques passives

- L'objectif est d'obtenir des informations sur une transmission d'informations
  - N'altère pas le message ou la communication
- Regroupe deux grands types d'attaque
  - L'écoute clandestine (eavesdropping)
  - Capture et analyse de trafic
- Très difficile à détecter

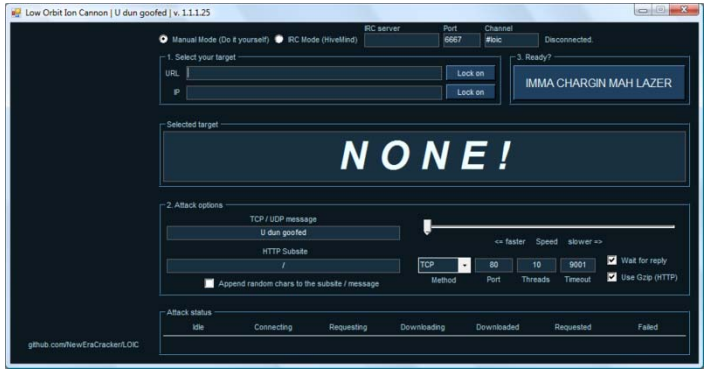


Les attaques actives

- A contrario, les attaques actives vont impliquer une altération de la communication
  - Usurpation d'identité (Masquerade ou spoofing)
    - Une personne se fait passer pour une autre en créant des données contenant de fausses informations
      - ★ *Peut être assimilé à de la contrefaçon*
    - Ex: ARP Spoofing, IP Spoofing…
  - Rejeu
    - Des traces préalablement capturées sont rejouées dans un but frauduleux
      - ★ *Obtenir un accès normalement interdit, obtenir des réponses pour déterminer un mot de passe (cf WEP)*
      - ★ *Incrémenter des revenus, …*
  - L'altération de messages
    - Modification des paquets d'une communication pour ajouter/supprimer/modifier l'information qu'il transporte

Les attaques actives

- Le déni de service
  - Envoie d'un très grand nombre d'informations (requêtes ou données) pour rendre le service inopérant
  - Relativement simples à mettre en œuvre (Ex: LOIC)



But des attaques

- Pour synthétiser, les attaques ont 4 objectifs principaux
  - L'interruption: qui vise la disponibilité des informations
  - L'interception: qui vise la confidentialité des informations
  - La modification: qui vise l'intégrité des informations
  - La fabrication: qui vise l'authenticité des informations

Prévention des attaques

- Les attaques passives sont difficiles à détecter mais simples à prévenir
  - Il faut donc mettre en place des mécanismes pour les prévenir
  - Ex: Cryptage de l'information et/ou du médium de communication
    - Cryptographie quantique pour détecter l'écoute

- Les attaques actives sont simples à détecter mais difficiles à arrêter
  - Il faut donc mettre l'accent sur la détection et sur la récupération
    - Bien entendu on ne néglige pas la prévention !
  - Ex: Firewall, Systèmes de détection d'intrusion, signatures, antivirus, sauvegardes…

Les mécanismes de sécurité

- Les mécanismes de sécurité désignent les moyens de défense pour
  - Détecter une attaque
  - Prévenir une attaque
  - Récupérer d'une attaque
- Un mécanisme de sécurité ne remplie jamais toutes les fonctions précédentes
- Quelques mécanismes
  - L'authentification
    - Mécanisme central qui est souvent utilisé par d'autres mécanismes (ex confidentialité)
    - Authentifier un acteur peut se faire à l'aide de trois aspects

★ *Ce qu'il sait* ⟶
⟵ ★ *Ce qu'il est*

★ *Ce qu'il possède* ⟶

    - Dans les domaines de communications on s'emploie surtout à identifier l'émetteur d'un message
      - ★ *Pour identifier le destinataire il faut mettre en place une double authentification*

Les mécanismes de sécurité

- Le chiffrement des données (encypherment)
  - Algorithmes à base de clés permettant de transformer les données
  - Le niveau de sécurité est dépendant de la sécurité des clés
- La signature des données
  - Données ajoutées aux informations transmises pour assurer l'authenticité du message
- Le contrôle d'accès
  - Au système (vérification des droits)
  - Au moyen de communication (VPN ou tunnels)
- Le contrôle du routage
  - Sécurisation des chemins empruntés et des mécanismes d'interconnexion
- Le bourrage de trafic
  - Des données sont ajoutées pour assurer la confidentialité en particulier au niveau du volume de trafic

Les mécanismes de sécurité

- La notarisation
  - Utilisation de tiers de confiance pour assurer certains services de sécurité
    - ★ *Horodatage*
    - ★ *Certification*
    - ★ *Distribution de clés*
    - ★ …
- La protection physique
  - Attention aux supports papiers…

Retour sur la chaine de confiance

- La confiance dans la sécurité d'un SI va être directement liée à la confiance que l'on a dans les systèmes qui le composent
  - Min(niveau de confiance des systèmes)
  - Les mécanismes de sécurités établissent la confiance
  - Dans le cas de systèmes répartis, le niveau de confiance va également considérer le canal de communication comme un système particulier
- La chaine de confiance repose sur un principe simple
  - Les amis surs de mes amis surs sont surs
- Pbm: qu'est-ce qu'un ami sur ?
  - Les organismes de certifications permettent de répondre à ce problème
  - Etablissement de graphes de confiance
    - Plus il y a d'échanges surs plus la confiance grandie
  - Il faut néanmoins toujours avoir la possibilité de révoquer la confiance accordée

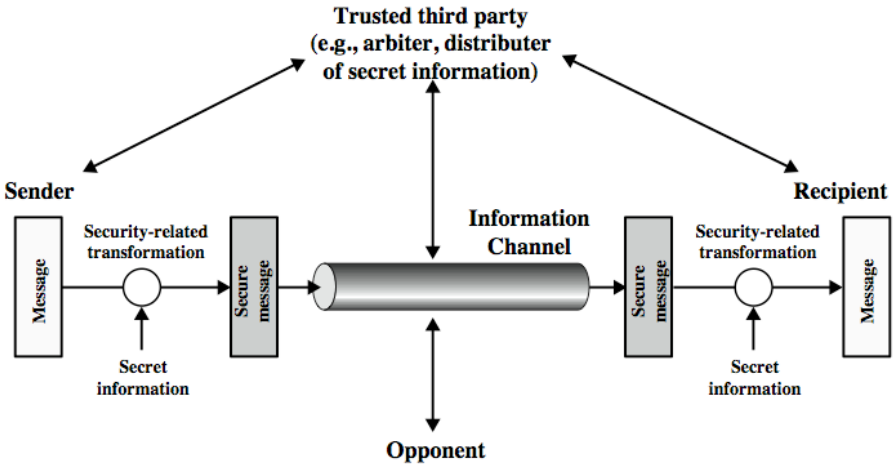
Les services de sécurité

- Les services de sécurité définis dans X.800 s'appuient sur les mécanismes précédents
- Ils sont au nombre de 5 et se rapprochent de la triade CID
  - Authentification
  - Contrôle d'accès
  - Confidentialité des données
  - Intégrité des données
  - Non répudiation des données

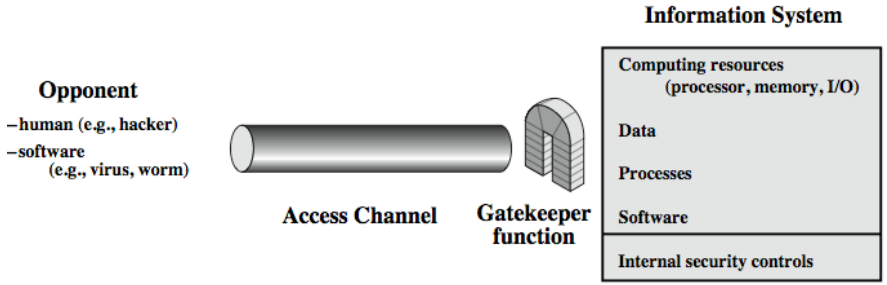
Relations entre services et mécanismes de sécurité

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Un model pour la sécurité réseau



Un model pour la sécurité des accès réseaux



Le principe du moindre privilège

- Tout ce qui n'est pas explicitement autorisé est interdit
- Il ne faut autoriser que ce qui est utile et justifié par les taches de l'utilisateur
  - Attention néanmoins à ne pas tomber dans l'excès
    - Une règle trop restrictive a tendance à être contournée
  - L'ergonomie doit être préservée
    - Il ne faut pas demander un mot de passe tous les clicks
- Exemple souvent utilisé par les responsables réseaux:
  - On bloque tous les ports de communications sauf ceux expressément autorisés
    - SMTP, POP, HTTP…

La défense en profondeur

- Consiste à utiliser plusieurs techniques de sécurités parfois redondante pour arrêter/ralentir l'attaquant

- Exemple
  - Un antivirus sur le serveur de mail et un autre sur chaque poste client
  - Un pare-feu à l'entrée du réseau et au niveau de chaque serveur