Année 2008-2009

esil

Sécurité des systèmes informatiques
— Introduction —

Nicolas Baudru
mél : nicolas.baudru@esil.univmed.fr
page web : nicolas.baudru.esil.perso.univmed.fr

Système d'information et système informatique

esil

Système d'information : ensemble des moyens nécessaires pour acquérir, stocker, exploiter . . . des informations

Système informatique : un des moyens techniques pour faire fonctionner un système d'information

➥ Pour assurer la sécurité d'un système d'information, il faut assurer la sécurité du système informatique.

Sécurité informatique : ensemble des moyens mis en oeuvre pour minimiser la vulnérabilité d'un système informatique contre des menaces

Menaces

esil

Menaces passives : consistent à écouter ou copier des informations de manière illicite
Des menaces actives : consistent à altérer des informations ou le bon fonctionnement d'un service

Menaces dues aux accidents : ($<$30% des causes) incendies, inondations, pannes d'équipements, catastrophes naturelles...
Menaces dues à la malveillance : ($>$60%, en croissance, souvent d'origine interne) vols d'équipements, copies illicites, sabotage matériel, attaques logiques, intrusion et écoute, actes de vengeance...

Dans ce cours, nous aborderons uniquement les problèmes de sécurité informatique liés aux actions malveillantes

Les services de sécurité à assurer

esil

Cas d'un système informatique en réseaux :

☞ Des menaces :

- divulgation des données
- modification, destruction de données
- refus de service

☞ Des exigences de sécurité :

- confidentialité des données
- intégrité des données
- disponibilité de services
- authentification des utilisateurs et contrôle d'accès local

Les services de sécurité à assurer

esil

Cas d'un système informatique en réseaux :

☞ Des menaces supplémentaires :

- écoute passive, analyse du trafic
- rejeu
- modification, destruction de messages
- génération de trafic

☞ Des exigences supplémentaires :

- authentification du correspondant et de l'origine des données
- non-répudiation
- contrôle d'accès aux services offerts via le réseau

Vulnérabilité informatique

esil

Vulnérabilité : erreur de conception (bug) dans un produit pouvant altérer la sécurité du système

Où peut-on trouver des vulnérabilités ?

- au niveau du système d'exploitation
- au niveau applicatif
- au niveau du réseau

Vulnérabilité des systèmes informatiques isolés

esil

☞ Personnes utilisant le système :

- les utilisateurs légitimes ;
- les administrateurs ;
- les attaquants (crackers) qui peuvent être des utilisateurs légitimes.

☞ La diversité des utilisateurs d'un système pose certains problèmes :

- l'OS est utilisé par des personnes faillibles ;
- augmenter la sécurité implique souvent un manque de flexibilité et de convivialité.

➥ la gestion de la sécurité devient de plus en plus difficile pour l'administrateur.

Vulnérabilité des réseaux

esil

☞ Principales causes :

- les données transitent d'une machine à une autre dans un milieu non sécurisé/sécurisable (internet).
- failles applicatives de certaines piles de protocoles TCP/IP.
- mécanisme d'authentification insuffisant (ex : rsh, rlogin).

☞ Principales solutions mises en oeuvre :

- utiliser des méthodes de chiffrement.
- corriger les failles applicatives de piles des protocoles.
- filtrer les accès aux différents services.

Vulnérabilités informatiques

esil

Qui trouve des vulnérabilités ?

- des “chercheurs en vulnérabilités” indépendants (Vulnerability Contributor Program d'iDEFENSE, fondation Mozilla, ...)
- des “chercheurs en vulnérabilités” dont c'est le métier, (eEye, NGS, ISS, Core-ST, Symantec, ...)
- plus rarement les éditeurs de logiciels.

Comment trouver les vulnérabilités ?

- Audit de code source
- Tests sur le produit
- Reverse-engineering
- etc.

De la vulnérabilité à l'exploit

esil

Que faire ensuite ?

Il faut avertir l'éditeur ou l'équipe de développement de la vulnérabilité, puis attendre un correctif. Un bulletin de sécurité est ensuite publié.

Attention ! parfois une vulnérabilité est publiée sans que l'éditeur n'en soit averti, ou reste gardée secrète pour une utilisation malveillante.

Conduite à tenir face aux vulnérabilités

- Se tenir informé des nouvelles vulnérabilités
- Appliquer les correctifs
- Désactiver la fonctionnalité générant la vulnérabilité

Les exploits :

Ce sont des programmes permettant de tester une vulnérabilité, en tentant de l'exploiter. Ils sont écrits par le découvreur de la vulnérabilité ou par des indépendants, en se basant sur les détails fournis dans l'avis initial. L'exploit est ensuite ajouté à un scanner de vulnérabilité pour tester l'efficacité du correctif.

Thèmes abordés dans ce cours

esil

1. La cryptographie pour la sécurité
2. Attaques par escalade des privilèges
3. Attaques par deni de services