Cryptographie et sécurité des systèmes informatiques

Olivier Markowitch

Plan du cours

1. La principes de sécurité informatique
2. Le chiffrement symétrique
3. Le chiffrement asymétrique
4. L'intégrité
5. L'identification
6. Les signatures digitales
7. Les protocoles d'échange de clés
8. L'analyse de risques et plan de sécurité

Sécurité

Sécurité = besoin, cryptographie = outils

Politique de sécurité considèrant les aspects physiques et logiques

Réalisation d'une analyse de risques :
- prévention, détection et réaction
- confidentialité, intégrité et disponibilité

Attentions aux coûts (nouvelles ressources, modification de la manière de travailler, gestion de la sécurité)

Sécurisation

1. *Que veut-on sécuriser ?*

2. *Quel niveau du système informatique désire t'on sécuriser ?*

3. *Quel degré de complexité est acceptable ?*

4. *La sécurisation devra t'elle être centralisée ou distribuée ?*

5. *Quel mécanisme pour se protéger d'un attaquant tentant d'avoir accès à un niveau du sytème (cf question 2) qui est en-deçà des mécanismes sécuritaires ?*

11 principes sécuritaires ...

... à l’usage des concepteurs et administrateurs :

1. Un système parfaitement sûr n’existe pas

2. Un système sûr peut être cher

3. Minimiser le nombre, l’importance et la complexité de composants du système dans lesquel il faut être « aveuglément » confiants

4. Concevoir des mécanismes sécuritaires les plus simples possibles

5. Multiplier les niveaux de sécurité

Principes sécuritaires (suite)

6. Pas de sécurité par l'obscurité

7. Donner à chaque utilisateur les privilèges juste nécessaires à l'accomplissement d'une opération autorisée, ni plus, ni moins

8. Simplicité d'usage

9. Etre sceptique et paranoïaque

10. Définir une politique d'usage

11. Eduquer les utilisateurs du système

Remarque sur la sécurité physique

– Tempest : utilisation des émissions électromagnétiques émanant d'un PC

  M.G. Kuhn and R.J. Anderson" *Soft Tempest : Hidden Data Transmission Using Electromagnetic Emanations*. Lecture Notes in Computer Science, volume 1525, Springer 1998

– « Wiretapping » : techniques tentant d'intercepter des communications. Pour les cables : « paquet sniffing » ou inductance

Identification

L’identification est nécessaire, entre autres, au contrôle d’accès (prévention) et à l’analyse des fichiers de logs (détection)

Ambiguité dans le vocabulaire : identification, intégrité, authentification (d’entités et de données)

Technique la plus répandue : login et mot de passe

Identification : mots de passe

Risques :

– un même utilisateur utilise souvent le même mot de passe pour accéder à diverses ressources
– retenir $<>$ deviner

Attaques :

– onlines (fake login, attaques sociales)
– offlines (recherches exhaustives ou par dictionnaire)

Défenses : longueur minimum, format, généré automatiquement, expiration, limite essais, affichage informations, attaque par dictionnaire, salting, shadowing, trusted path, etc.

Identification : one-time password

Il est très fréquent qu'un mot de passe circule en clair sur le réseau lors d'une connexion distante

Le système d'indentification SKey est une solution à ce problème

Neil Haller *The S/Key one-time password system*. Symposium on Network and Distributed Systems Security, 1994

Ce système fait l'objet d'une standardisation internet RFC 1760.
ftp ://ftp.internic.net/rfc/rfc1760.txt

Identification

Peut-être basé sur :

- un secret
- possession
- identitié physique
- comportement
- etc.

Contrôle d'accès : définitions générales

Formellement nous avons :

- S un ensemble de sujets
- O un ensemble d'objets
- A un ensemble d'opérations d'accès
- M une matrice de contrôle d'accès

$M = (M_{s,o})_{s \in S, o \in O}$ et $M_{s,o} \subset A$

Une ligne de la matrice correspond à un utilisateur et s'appelle parfois en anglais « capabilities »

Une colonne de la matrice correspond à un objet et s'appelle parfois en anglais « access control list » (ACL)

Modèle de sécurité : Bell-Lapadula

$C(s)$: niveau de sécurité d'un sujet (clearance level)

$C(o)$: niveau de sécurité d'un objet (classification level)

Propriété simple : un sujet s peut avoir accès en lecture à un objet o si et seulement si $C(o) \leq C(s))$

Propiété $*$: un sujet s qui a accès en lecture à un objet o ne peut avoir accès en écriture à un objet p que si et seulement si $C(o) \leq C(p)$

Modèle de sécurité : Bell-Lapadula

Un état dépend d'un sujet, d'un objet, de leur niveau de sécurité respectif et du contenu de la cellule correspondante dans la matrice de contrôle d'accès

Un état est sûr s'il respecte les deux propriétés

Problèmes :
- uniquement la confidentialité
- matrice de contrôle d'accès statique
- covert channel

Modèle de sécurité : Biba

$I(s)$: niveau d'intégrité d'un sujet

$I(o)$: niveau d'intégrité d'un objet

Propriété simple : un sujet s peut modifier un objet o si et seulement si $I(o) \leq I(s)$

Propiété $*$: un sujet s qui a accès en lecture à un objet o ne peut avoir accès en écriture à un objet p que si et seulement si $I(p) \leq I(o)$

Autres modèles de sécurité

– Harrion - Ruzzo - Ullman (intégrité et confidentialité)

– Chinese Wall (intégrité et confidentialité)

– Clark - Wilson (intégrité)

D.F. Sterne *On the buzzword 'Security policy'*. Proceedings of the 1991 IEEE Symposium on research in security and privacy

H.J. Smith *Privacy policies and practices : inside the organisational maze*. Communication of the ACM 36(12), décembre 1993

J. McLean *Security models*. Encyclopedia of software engineering. Wiley & Sons, 1994

Evaluation de la sécurité

Evaluation d'applications ou de systèmes d'exploitation

Etapes : évaluation, certification, accréditation

Evaluation sur base de critères

Orange book ou TCSEC (Trusted Computer System Evaluation Criteria) : USA

ITSEC (Information Technology Security Evaluation Criteria) : France, Allemagne, Royaumes Unis, Pays Bas.

Evaluation de la sécurité : Orange Book

7 classes de sécurité définies itérativement par dégré croissant de précision

– D (minimal protection) : produit ou système qui ne rencontre aucun des critères de l'Orange Book

– C1 (discretionary security protection) : un utilisateur peut décider ce qui doit être contrôlé. Les utilisateurs doivent être identifiés par le système, les utilisateurs sont séparés en terme de données

– C2 (controlled access protection) : comme en C1, les utilisateurs sont responsables de leurs actions avec une granularité de contrôle plus fine. Mise en place d'audit des actions des utilisateurs sur chacun des objets du système

Evaluation de la sécurité : Orange Book

– B1 (labelled security protection) : contôle d'accès non à discretion des utilisateurs. Tous les objets contrôlés et tous les sujets sont assignés à un niveau de sécurité. Tous les objets ne doivent pas être contrôlés en B1. Chaque objet contrôlé et sujet possède un label indiquant ce niveau de sécurité. Ce label sera utilisé lors du contrôle d'accès. La police de contrôle d'accès doit implémenter le modèle de Bell-La Padula

– B2 (structred protection) : un design de haut niveau (conceptuel) vérifiable doit être présenté, ainsi qu'un test confirmant que le système ou produit implémente ce design. Le système ou produit doit être conçu en modules indépendants. Une analyse des « covert channels » doit être réalisé

Evaluation de la sécurité : Orange Book

- B3 (security domain) : le management du système ou produit doit permettre l'audit et la récupération des données (« recovery »). Chaque fonctionnalité de sécurité doit pouvoir être complètement testée. En plus des tests, une argumentation formelle montrant que le système ou produit respecte le design doit être présenté

- A1 (verified design) : le design est entièrement vérifié formellement. Il faut :
  - un modèle formel du système de protection et la preuve de sa consistance
  - une spécification formelle des fonctionnalités de haut niveau du système de protection
  - une preuve de la correspondance du modèle et la spécification
  - montrer informellement que l'implantation du système de protection est consistant avec la spécification
  - une analyse formelle des « covert channels »

Evaluation de la sécurité : ITSEC

Effectiveness (quoi) séparé de la correctness (comment)

Effectiveness évalue les adéquations du produit avec les besoins, la synergie avec les autres fonctionnalités, la robustesse et la simplicité d'usage. Cotations entre F1 et F10

La correctness évalue le processus de développement, l'environnement de développement, la documentation et la configuration du produit. Cotations entre E0 et E6

Evaluation de la sécurité : ITSEC

10 classes de fonctionnalités

Classes 6 à 10 non incrémentales mais spécifiques

– F1 $\rightarrow$ F5 : correspond respectivement aux fonctionnalités décrites dans les classes D $\rightarrow$ A1 de l'Orange Book

– F6 : haute intégrité

– F7 : haute disponibilité

– F8 : intégrité des données au cours de communications

– F9 : haute confidentialité

– F10 : réseau avec hautes confidentialité et intégrité

ITSEC (suite)

- E0 : assigné aux TOE qui échouent à l'évaluation
- E1 : description informelle du TOE et tests de la correspondance du TOE avec son but sécuritaire
- E2 : E1 + une description informelle du design doit être fourni
- E3 : un design détaillé et les codes sources des fonctions sécuritaires doivent être fournis. C'est le niveau le plus habituel
- E4 : un modèle formel de la police de sécurité ainsi qu'une analyse rigoureuse des vulnérabilités doit être fourni
- E5 : établissement des correspondances entre le design détaillé et le code source. L'analyse des vulnérabilités se base dés lors sur le code source
- E6 : description formelle de l'architecture sécuritaire et la vérification de la consistance vis à vis du modèle formel de la police de sécurité doivent être fournis

Correspondance ...

... entre l'Orange Book et ITSEC :

- D $\leftrightarrow$ E0
- C1 $\leftrightarrow$ F1 + E2
- C2 $\leftrightarrow$ F2 + E2
- B1 $\leftrightarrow$ F3 + E3
- B2 $\leftrightarrow$ F4 + E4
- B3 $\leftrightarrow$ F5 + E5
- A1 $\leftrightarrow$ F5 + E6

Réseaux : IPSEC

Le stack TCP-IP peut être modifié pour y intégrer des mécanismes sécuritaires

Security architecture for IP (RFC 1825, 26 et 27)

Modification du stack basée sur IP : ajoute des mécanismes assurant l'intégrité et la confidentialité

Application
Transport & Session (TCP)
IPSEC
Interface

L'interface habituelle à IP $\rightarrow$ couches supérieures ne changent pas

N. Doraswamy et D. Harkins *IPSec : the new security standard for the Internet, Intranets, and Virtual Private Networks*. Prentice-Hall, 1999 (ISBN :0-13-011898-2)
http ://www.phptr.com/ptrbooks/ptr_0130118982.html

Réseaux : Secure socket layer

SSL : Netscape et repris par IETF sous le nom de « Transport layer security » (TLS)

Application
SSL
TCP
Internet (IP)
Interface

Ajoute à TCP des mécanismes d'intégrité et de confidentialité, les applications doivent explicitement faire appel aux mécanismes de sécurité

K.E.B. Hickman et T. Elgamal *The SSL Protocol*. RFC draft, Netscape Communications Corp. 1995

ISO *Telecommunications and Information Exchange Between Systems - Transport Layer Security Protocol*. International Standards Organization, ISO/IEC JTC1/SC6 N6794

La protection du réseau

le firewall utilise :

1. le packet filtering : mécanisme qui lit les headers des paquets de données et vérifie éventuellement :

– l’adresse source

– l’adresse destination

– le protocole utilisé

– le type de connexion

La protection du réseau

le firewall utilise :

2. un serveur proxy qui :

– intercepte les requêtes provenant du réseau interne et décide s'il la laisse passer ou non sur base de règles définies
– impersonnalise l'émetteur de la requête vis à vis du monde extérieur (cette opération est transparente pour l'émetteur)
– réalise le logging

Le serveur proxy peut être précis et peut accepter un protocole mais limiter les opérations au sein du protocole (par exemple permettre ftp mais empêcher get). Un tel serveur proxy est nécessaire par application existante.