Menaces & Vulnérabilités

Yannick Chevalier
Université de Toulouse
CSA M1, Security

Plan

Protéger de qui ?

Ce qu'on a vu

1. décomposition : on définit la sécurité par l'absence d'influence anormales
2. niveaux de protection : on définit les influences normales et celles qu'il faut contrôler
3. contrôle d'accès/authentification : on définit les personnes aux frontières du SI

Aujourd'hui

- définition des menaces, attaques, et autres
- tour d'horizon de ce qui existe en terme d'attaques
- définition des attaquants possibles

Plan

1. Vulnérabilité
2. Menace
3. Attaque

VULNÉRABILITÉS

POINT DE VUE ABSTRAIT

flux d'information anormal possible et pas traité par une procédure de classification/déclassification (entre les composants) ni par le contrôle d'accès (pour les sujets)

POINT DE VUE CONCRET

Essentiellement deux cas possibles :

VULNÉRABILITÉS

POINT DE VUE ABSTRAIT

flux d'information anormal possible et pas traité par une procédure de classification/déclassification (entre les composants) ni par le contrôle d'accès (pour les sujets)

POINT DE VUE CONCRET

Essentiellement deux cas possibles :

- Y'a un bug : l'exploitation d'un bug permet des flux d'information non prévus

VULNÉRABILITÉS

POINT DE VUE ABSTRAIT

flux d'information anormal possible et pas traité par une procédure de classification/déclassification (entre les composants) ni par le contrôle d'accès (pour les sujets)

POINT DE VUE CONCRET

Essentiellement deux cas possibles :

- Y'a un bug : l'exploitation d'un bug permet des flux d'information non prévus
- Y'a un trou dans le mur : tous les cas n'ont pas été recensés, ou certains recensés ont été mal traités

MENACE

DÉFINITION

toute chose ou personne dont l'effet est un dommage au système à protéger

EXEMPLES

- pluie si une partie du site est en zone inondable
- employé mécontent
- concurrent

suite : focus sur les menaces représentées par des humains

Attaque

Définition

Une attaque de sécurité est l'exploitation d'une vulnérabilité par un acteur (personne, entreprise, État)

Points à considérer

- concrétisation d'une menace humaine
- buts (gain *vs.* perte) et opportunité (facilité à mener une attaque) à prendre en compte dans la mesure de dangerosité

Il est important d'identifier les acteurs possibles

Plan

VULNÉRABILITÉS LOGICIELLES

CAS NON TRAITÉS

- pas d'analyse de sécurité spécifique
- analyse de sécurité partielle

VULNÉRABILITÉS LOGICIELLES

CAS NON TRAITÉS

- pas d'analyse de sécurité spécifique
- analyse de sécurité partielle

ERREURS DANS LE SYSTÈME DE SÉCURITÉ

- erreur de conception
- erreur d'implémentation

Analyse de sécurité partielle

Modèle

Système à sécuriser = graphe :

- les nœuds sont les composants
- les arcs sont les flux d'information entre composants

Pour la personne protégeant le SI :

- vue du SI composant par composant
- focus sur les arcs menant aux composants les plus importants
- manque de moyens : oubli des autres

Pour une personne attaquant le SI

- les attaques directes sont rares !
- en général : compromissions successives de composants du SI
- un attaquant recherche d'un chemin dans le graphe qui l'amène d'un nœud contrôlé vers un nœud but

Erreurs de conception

Protocoles

- hypothèses non raisonnables (*e.g.*, cryptographie parfaite)
- erreurs logiques dans la spécification du protocole (*cf.* TD)

Contrôle d'accès

- erreurs dans l'écriture de la politique de contrôle d'accès

  Pour certains systèmes d'entreprises, une politique pouvant être décrite en quelques lignes demande des pages d'écriture de règles

- erreurs dans les règles de filtrage des pare-feux

Morale

- la conception de composants pour la sécurité demande une grande expertise
- toujours préférable de réutiliser des solutions existantes

Erreurs d'implémentation (1/2)

Erreurs logicielles

- heartbleed : attaque sur une implémentation de TLS
- buffer overflow
- ...

Contre-mesures

- utilisation de flags lors de la compilation (pour gcc, `-fstack-protector-strong` alerte en cas de buffer overflow)
- relecture de code, documentation, ingénierie logicielle

Erreurs d'implémentation (2/2)

Erreurs spécifiques à la sécurité

- mise à zéro d'un tableau enlevée lors de l'optimisation
- différences de temps d'exécution dans différents cas qui permettent de remonter aux valeurs dans un programme
- $\Rightarrow$ certaines failles ne sont pas capturables par le développement logiciel classique

Contre-mesures

Utilisation de code développé par des experts (par exemple, libsodium)

Plan

Importance

De la vulnérabilité à l'attaque

opportunité d'exploitation d'une vulnérabilité dépend :

- des possibilités d'accès des acteurs possibles
- gain possible de cette exploitation pour chaque acteur identifié
- mitigé par le coût anticipé de cette exploitation pour chaque acteur identifié

Identification d'une menace

- qui : quelle puissance de calcul ? quel accès de base donné par le système de contrôle d'accès ?
- pourquoi : balance des risques : gains *vs* perte
- but : au sein du SI ou au-delà ?

Qui ?

	puissance	accès	risques
état	+++	+++	+
concurrent	++	+	++
employé	+	+++	+++
cyber-crime	+ à ++	+ à ++	+

Remarques :

- peu de rétorsions possible contre un état étranger, l'accès direct est en général faible
- un concurrent peu avoir (par des relations communes) accès à certaines données, rétorsions contre un concurrent étranger faibles
- un employé part avec beaucoup plus de données, mais n'a pas beaucoup de moyens

Sécuriser en augmentant les risques/la difficulté

Raisonnement

Si la menace est motivée par un rapport bénéfice/coût, on peut augmenter le coût pour réduire l'opportunité de mener l'attaque

Exemples

- logs, surveillance vidéo : preuve d'implication d'une personne
- cryptographie : obligation de mise en œuvre de moyens chers
- fouille, sas, carte d'identité : contournements chers

Mais...

- la mise en place de solutions de sécurité coûte cher
- audit : valider le coût d'une solution par rapport à la perte causée par une attaque
- exemple : pendant longtemps, attaque connue (et utilisée) mais non corrigée sur les cartes bleues car la solution aurait coûter plus cher que la fraude

Dans quel but ?

Dans le cadre du recensement des composants

- ressources interne à protéger (cartes d'accès, données de l'entreprise)
- ressources permettant d'accéder à des ressources externes (vol de cartes d'identités vierges chez un imprimeur)
- cloud : le rôle de l'hébergeur est aussi de sécuriser les données de ses clients

Évaluation des moyens pouvant être mis en œuvre

- coût $<$ bénéfices potentiels
- évaluation par rapport aux accès possibles, pas par rapport au statut (la RDA visait principalement les secrétaires pour obtenir des informations, pas les haut-fonctionnaires)

Fraude interne

Catégories de fraudeur

occasionnel, récurrent (de petites sommes à chaque fois), professionnel (se fait embaucher pour commettre une fraude), organisé (en groupe)

Vulnérabilités

faibles procédures de contrôle interne et de surveillance des opérations, contrôle d'accès trop permissif, absence de séparation de tâche

Fraudes recensées

détournement des avoirs de la clientèle ou de l'entreprise, création de fausses opérations, falsification des objectifs pour un gain de rémunération

Plan

cf. TD