Sécurité pratique

Chapitre 1: Concepts et terminologie

Printemps 2022

Prof. Marcelo Pasin

haute école
neuchâtel berne jura
arc ingénierie
www.he-arc.ch

Concepts et terminologie

- Concepts et vision globale
- Menaces et attaques
- Principes fondamentaux
- Gestion et stratégies de sécurité

Objectifs d'apprentissage

Être capable de

- Expliquer les principes fondamentaux de la sécurité
- Stipuler des menaces et des attaques à traiter
- Décrire des besoins de confidentialité, d'intégrité et de disponibilité
- Débattre à propos des surfaces d'attaque
- Comprendre quelques stratégies de sécurité

Concepts et vision globale

Définition

- **Sécurité : mesures et contrôles pour assurer confidentialité, intégrité et disponibilité d'atouts***

- **Confidentialité** : respect des contraintes d'accès
- **Intégrité** : préservation de l'état de l'information
  - Modification, suppression
- **Disponibilité** : préservation des fonctionnalités
  - Y compris leur temps de réponse (*availability*)

* **Atouts** (*assets*)
  - **Ressources** matériels et logiciels
  - Information traitée, stockée et communiquée

Autres aspects de la sécurité

- **Authenticité**
  - Il est possible de vérifier si l'atout est authentique
- **Non-répudiation**
  - Un fait réel ne peut être nié
- **Responsabilisation** (*accountability*)
  - Il n'est pas possible de cacher des actions du passé (ni les acteurs)

Impacte et risque

- Niveau d'**impacte** d'une faille de sécurité
  - Bas : le dégât a une taille connue, limitée, souvent réversible
  - Moyen : le dégât aurait un réel effet négatif
  - Haut : dégât catastrophique, grand en taille, irréversible
  - Ce n'est pas la même chose que la probabilité !
- Niveau de **risque**
  - Mesure dans laquelle un atout est menacé par une attaque potentielle
  - Typiquement, une fonction de
    - L'adversité de l'impacte de l'attaque
    - La probabilité de l'occurrence de l'attaque

Atouts

- Types d'atouts, de ressources (*assets*)
  - Matériels
    - Ordinateurs
    - Dispositifs de stockage
    - Dispositifs de réseau
  - Logiciel
    - Système
    - Applications
  - Données
    - Fichiers, bases de données
    - Données de la sécurité (fichier de mots-de-passe par exemple)

Menaces

- Menace (*threat*)
  - Circonstance ou évènement ayant un impacte potentiel
- Adversaire (agent menaçant)
  - Personne (ou groupe) qui mène ou a l'intention de mener des activités nuisibles

- Menace persistante avancée (*advanced persistant threat*)
  - Acteur furtif de menace de réseau informatique
  - Généralement un État national (ou parrainé par un état)
  - Intrusions ciblées, à grande échelle, avec objectifs spécifiques
    - Les APT réussisent des attaques prolongées et non détectées

Vulnérabilité et attaque

- Vulnérabilité
  - Faiblesse exploitable par un adversaire
  - Dérivée d'une menace
  - Types: corruption, fuite (*leak*), indisponibilité
- Attaque
  - Tout type d'activité malveillante pour observer, collecter, perturber, dégrader, voler, détruire (etc.) des ressources informatiques ou l'information elle même.
- Contre-mesure
  - Un dispositif ou une technique pour réduire l'efficacité d'une action indésirable

Les défis de la sécurité (1)

- La sécurité est contre-intuitive pour les utilisateurs
  - Seul l'étude détaillée des menaces donne un sens aux mécanismes
- Nombreux utilisateurs (y compris des admins) perçoivent la sécurité comme un fardeau
- Il y a une tendance à ignorer la sécurité avant les premiers dégâts
- On pense à la sécurité comme une extension
  - Non pas comme une fonction de base, à concevoir avec le service
- Ce n'est pas un sujet simple pour un débutant
  - Les besoins semblent simples
  - Implémenter des mécanismes peut devenir très complexe

Les défis de la sécurité (2)

- Les mécanismes doivent être soigneusement conçus
  - Attaques exploitent les défaut des mécanismes, utilisation tordue
- La sécurité dépend d'un certain nombre de secrets
  - Il faut gérer les secrets (créer, stocker, transmettre)
- La localisation des mécanismes joue aussi un rôle
  - Une attaque physique pourrait battre une protection logicielle
- La sécurité demande une surveillance constante
  - Difficile avec un grand nombre de petites actions concurrentes
- La sécurité comporte une compétition déloyale
  - À l'attaquant, il suffit de trouver un défaut
  - L'administrateur doit éliminer tous défauts

Menaces et attaques

Attaque:
Divulgation non autorisée (*disclosure*)

- Conséquence
  - Une entité a accès à des données pour lesquelles elle n'est pas autorisée

- Actions
  - **Exposition**: des données sensibles sont directement transmises à une entité non autorisée
  - **Interception**: une entité non autorisée accède directement aux données sensibles transitant entre sources et destinations autorisées
  - **Inférence**: entité non autorisée accède indirectement à des données sensibles, à partir de caractéristiques ou de sous-produits de communications
  - **Intrusion**: une entité non autorisée accède à des données sensibles en contournant les protections

Attaque:
Tromperie, fraude (*deception*)

- Conséquence
  - Une entité autorisée reçoit de fausses données et qu'elle les croit vraies

- Actions
  - **Mascarade**: une entité se fait passer pour une autre
  - **Falsification**: utiliser des fausses données
  - **Répudiation**: nier faussement sa responsabilité

Attaque: Perturbation (*disruption*)

- Conséquence
  - Circonstance ou événement interrompt ou empêche le bon fonctionnement d'un service ou de ses fonctions

- Actions
  - **Incapacité**: empêcher ou interrompre le fonctionnement d'une ressource en désactivant un de ses composants
  - **Corruption**: altérer de manière indésirable le fonctionnement d'une ressource en modifiant de manière nuisible ses fonctions ou ses données
  - **Obstruction**: interrompre la fourniture du service en empêchant son fonctionnement ou son accès

Attaque: Usurpation

- Conséquence
  - Une circonstance ou un événement entraîne le contrôle d'une ressource ou de ses fonctions par une entité non autorisée

- Actions
  - **Détournement**: prendre le contrôle non autorisé d'une ressource système (*misappropriation*)
  - **Mauvaise usage**: faire un composant de la ressource exécuter une fonction nuisible à sa sécurité

Exemples de menaces à la disponibilité

- Matériel
  - Un ordinateur est volé ou éteint
  - Un câble réseau est coupé
- Logiciel
  - Un programme est effacé
- Données
  - Fichiers sont effacés
  - Des données dans un fichier sont effacées
- Communication
  - Des messages du réseau sont supprimés

Exemples de menaces à la confidentialité

- Matériel
  - Un écran est observé (ou filmé)
  - Une clé USB est volée
- Logiciel
  - Le logiciel est copié (piraté)
- Données
  - Une donnée est lue sans autorisation
  - Une analyse statistique permet d'inférer sur des données
- Communication
  - Les contenus des messages du réseau sont observées
  - Le pattern des messages est observé

Exemples de menaces à l'intégrité

- Matériel
  - Un disque dur est remplacé
  - Un disque dur est endommagé
- Logiciel
  - Un programme est modifié
- Données
  - Fichiers sont modifiés
  - Fichiers sont remplacés
- Communication
  - Des messages du réseau sont modifiés
  - … retardés
  - … falsifiés

Attaques du réseau

- Attaques passives
  - Écoute (*eavesdropping*)
  - Analyse du traffique

- Attaques actives
  - Répétition (*replay*)
  - Mascarade (*masquerade*)
  - Altération (*tampering*)
  - Déni de service

Surface d’attaque

- Vulnérabilités atteignables et exploitables

Exemples

- Ports réseau ouverts au monde extérieur
  - Services qui répondent à ces ports
- Des services dans un firewall
- Des services qui traitent des données externes (email, documents Word, etc.)
- Des services particuliers (SQL, applications web, etc.)
- Un employé avec accès à l’information sensible
  - Vulnérable à l’ingénierie sociale

Analyse de la surface d'attaque

- L'analyse de la surface d'attaque est une technique
- Évaluer l'échelle et la sévérité des menaces

- Aide à déterminer
  - Des points où la sécurité doit être renforcée
  - Des points où diminuer la surface d'attaque
  - Quelle partie du système doit être modifiée

Catégories de surfaces d'attaque

- Réseau
  - Les vulnérabilités des protocoles
  - *Denial-of-service*
  - Interruption des liens de communication
  - Attaques par intrusion
- Logiciel
  - Vulnérabilités du code des services
  - Un type très spécial : les services web
- Humain
  - Personnel et outsiders
  - Erreur humaine
  - Social engineering

Les principes de la sécurité

Principes de la conception sécurisée

- Economie des mécanismes
- Sûreté à l'omission
- Médiation complète
- Conception ouverte
- Séparation des privilèges
- Moindre privilège
- Moindre fonction commune
- Acceptabilité psychologique
- Isolation
- Encapsulation
- Modularité
- Superposition
- Moindre étonnement

Économie des mécanismes

- La sécurité doit être simple et petite
  - Plus facile à tester et à vérifier de manière approfondie
  - Probablement moins de faiblesses subtiles
  - Moins de maintenance, mise à jour, remplacement
  - Gestion et configuration simplifiée
- Principe difficile à respecter
  - Demande constante de nouvelles fonctionnalités
- Garder ce principe à l'esprit lors de la conception
- Éliminer toute complexité inutile

Sûreté par omission (*fail-safe default*)

- Accès contrôlé par permission plutôt que sur par exclusion
- Pas d'accès garanti par omission
- On identifie des conditions pour autoriser l'accès
- Meilleur mode de défaillance que le contraire
- Erreurs (conception/mise en œuvre) rapidement détectées
  - Il passerait inaperçu dans la conception contraire
- Exemples: accès aux fichiers, client-serveur

Médiation complète

- Tout accès doit être vérifié
- Ne pas compter sur des décisions précédentes
- Approche gourmande en ressources

- Cas contraire: comment prendre en compte les changements ?
- Exemple:
  - L'ouverture d'un fichier entraine un contrôle d'accès
  - Lecture ou écriture possibles ensuite (sans contrôle)
  - Que faire si les permissions changent entre temps ?

Conception ouverte

- Le design doit être ouvert (non pas un secret)
- Des experts peuvent le réviser amplement
- La révision permet d'enlever des défauts
- Le mécanisme devient plus fiable

- Exemple :
  - L'algorithme de chiffrement est amplement connu
  - Ce sont les clés de chiffrement qui sont secrètes

Séparation des privilèges

- Plusieurs attributs sont nécessaires pour une tâche complète
- Chaque sous-tâche est contrôlée par un attribut différent
- Appropriation indue d'un attribut permet un dégât limité

- Exemples :
  - Authentification à plusieurs facteurs
  - Les privilèges d'administrateur d'un système d'exploitation

Moindre privilège

- Chaque action doit opérer avec un minimum de privilèges
- Ne pas donner des privilèges inutiles (en trop)
- Si possible, limiter aussi dans le temps
- Appropriation indue d'un privilège permet un dégât limité
- Exemple :
  - Contrôle d'accès associé aux rôles des utilisateurs
  - Chaque rôle a les privilèges nécessaires à ses tâches
  - Chaque accès particulier est explicitement accordé par un privilège spécifique

- Toute politique de contrôle d'accès doit accorder seulement des privilèges nécessaires

Moindre fonction commune

- Offrir des fonctions indépendantes à chaque rôle d'utilisateur
  - Minimum de fonctions partagées entre rôles
- Réduction du nombre de voies de communication entre fonctions
- Réduction de composants communs
- Plus facile à vérifier s'il y a des conséquences indésirables

Acceptabilité psychologique

- La sécurité ne doit pas changer la logique
- Les utilisateurs se passent d'une sécurité trop compliquée
  - La sécurité doit rester aussi transparente que possible
  - Minimum d'obstruction, comportement intrusif, fardeau
- Garder le modèle mental du service et de sa protection
- Si le changement est grand : l'utilisateur risque de se tromper

Moindre étonnement

- Les services doivent répondre comme attendu
- Comportement intuitif

Isolation

- Services en libre accès : isolés des services critiques
- Données d'un utilisateur : isolés des celles des autres
- Services de la sécurité : isolés tout court (sans accès)
- Systèmes d'exploitation ont des mécanismes d'isolation
- Isolation physique peut être envisagée

Encapsulation

- Type particulier d'isolation
- Orientation objet
- Chaque groupe de fonctions encapsule ses données
- Le contenu encapsulé n'est pas accessible de l'extérieur

Modularité

- Implémenter la sécurité dans des modules séparés
- Utiliser une architecture modulaire

- Réutilisation des modules
- Mise à jour et remplacement facilités

Superposition

- Des couches de protection
- Une faille à une couche ne compromet pas le tout

- *Layering*
- *Defense in depth*

Gestion de la sécurité

Gestion de la sécurité

- Planification et certification
- Responsabilité
- Contrôle d’accès
- Configuration et maintenance
- Protection physique
- Préparation aux incidents

Planification, certification et évaluation

- Plan de sécurité
  - Décrire les contrôles de sécurité en place ou planifiés
  - Définir les règles de comportement des utilisateurs
  - Développer, documenter, mettre à jour périodiquement

- Certification, accréditation et évaluations de sécurité
  - Évaluer périodiquement les contrôles de sécurité
    - Déterminer si les contrôles sont efficaces dans leur application
  - Élaborer et mettre en œuvre des plans d'action
    - Corriger les lacunes et réduire ou éliminer les vulnérabilités
  - Surveiller les contrôles de sécurité, assurer l'efficacité continue

Responsabilité

- Sensibilisation et formation
  - Informer et former responsables et utilisateurs
  - Traiter les risques et les responsabilités
  - Mentionner lois, réglementations et politiques en vigueur

- Audit et responsabilité
  - Créer, protéger et conserver des traces des actions et des acteurs
  - Surveiller, analyser, signaler et enquêter les actions indues

Contrôle d’accès

- Contrôle d'accès
  - Fixer des règes d'accès des
    - Dispositifs
    - Système d'information, services
    - Fonctions, transactions
  - Donner des droits individuels aux
    - Utilisateurs autorisés
    - Processus agissant à leur compte

- Identification et authentification
  - Identifier les utilisateurs et les processus agissant à leur compte
  - Authentifier (vérifier) les identités

Configuration et maintenance

- Gestion de la configuration
  - Établir et maintenir des configurations de base et des inventaires
  - Gérer des cycles de vie de développement des systèmes
  - Établir et appliquer des paramètres de configuration de sécurité

- Maintenance
  - Effectuer une maintenance périodique et ponctuelle
  - Assurer un contrôle efficace des outils et du personnel

Protection physique

- Protection des supports
  - Protéger les supports, papier ou numériques
  - Limiter l'accès de supports aux utilisateurs autorisés
  - Effacer (ou même détruire) les supports après utilisation

- Protection physique et environnementale
  - Protéger l'installation physique (y compris de l’environnement)
  - Limiter l'accès physique des ressources aux personnes autorisées
  - Prévoir des contrôles des installations

Préparation aux incidents

- Planification d'urgence (*contingency plan*)
  - Établir, maintenir et mettre en œuvre
    - Des plans d'interventions d'urgence
    - Des opérations de secours et de récupération après sinistre
  - But: garantir la disponibilité des ressources critiques

- Réaction à incidents
  - Établir une infrastructure de traitement des incidents
  - Préparer la détection, l'analyse, le confinement, la récupération
  - Organiser la réponse à l'utilisateur
  - Suivre, documenter et signaler les incidents aux responsables

Stratégies de sécurité

- Politique de sécurité, spécification
  - Qu'est-ce que la sécurité doit faire ?
- Implémentation, mécanismes
  - Comment faire ?
- Exactitude, assurance
  - Est-ce que ça marche ?

Spécification d'une politique

- Politique de sécurité
  - Ensemble de critères et contraintes
  - But: le maintien des conditions de sécurité

- Les facteurs à considérer
  - La valeur des atouts protégés
  - Les vulnérabilités du système
  - Les menaces potentielles, la probabilité des attaques
- Facilité x sécurité
  - La sécurité a toujours un prix en complexité
- Coût de la sécurité x coût de récupération
  - Choix de gestion (non pas technique)

Implémentation de la sécurité

- Prévention
  - Déterminer quelles menaces seront traitées
- Détection
  - Déterminer quelles menaces seront détectées
  - Quand la prévention n'est pas viable
- Réponse
  - Comment réagir en cas de détection
- Récupération
  - Une fois l'attaque arrêtée, comment réparer les dégâts
- Assurance
  - Déterminer quelles sont les garanties données par le système
  - Évaluation: analyse et test

Exemples de standards

- ISO/IEC 38500
  - Principes de gouvernance, senior management
- ISACA / COBIT (Control Objectives for Information and Related Technology)
  - Business goals x processes + IT
- ITIL (Information Technology Infrastructure Library)
  - Ensemble de bonnes pratiques
- ISO/IEC 20000
  - Ensemble de règles pour la gestion de services de TI
- NIST / CSF (Cybersecurity Framework)
  - Cadre de référence de l'état américain

Bilan

- Nous avons vu ce que c'est la sécurité
  - Confidentialité, intégrité, disponibilité
    - Aussi authenticité, non-répudiation, responsabilisation
- Nous avons connu quelques attaques et quelques menaces
- Nous avons connu les principes de la sécurité informatique
- Nous avons appris (un tout petit peu) à propos de la gestion de la sécurité

Suite

1. Concepts, terminologie

2. Malware, attaques
3. Cryptographie
4. Authentification et contrôle d’accès
5. Ethique et loi