Introduction à la Securité des Systèmes d'Information

Matthieu Herrb

IMT Mines Albi, 6 décembre 2023

http://homepages.laas.fr/matthieu/talks/intro-ssi-imt.pdf

Licence

Agenda

Agenda

Introduction

- Société de plus en plus dépendante aux systèmes informatiques
- Enjeux financiers croissants
- Attire les criminels
- Et donc nombre d'« attaques » en hausse

En face :

- Contraintes de coûts : sécurité pas toujours prise en compte au départ
- Historique : absence de culture de la sécurité (vs aéronautique)
- L'industrie de la sécurité des systèmes d'information intervient à posteriori

Définitions

On définit la sécurité de l'information par quatre critères :

Confidentialité : information connue uniquement des personnes autorisées

Disponibilité : information accessible aux personnes qui en ont besoin

Intégrité : information non modifiée sans autorisation

Traçabilité : conservation de l'historique des accès (lecture ou écriture) à l'information

Besoins de sécurité = évaluation du besoin pour chacun de ces critères.

Agenda

Vulnérabilités informatiques

- Problèmes de conception
- Mauvaises configurations
- Bugs (erreurs dans l'implémentation) $\rightarrow$ exploitables
- Facteurs humains

Problèmes de conception

- Collecte et stockage de données sensibles alors que cela n'est pas utile
- Stockage de données sensibles (mots de passe, identifiants bancaires...) en clair
- Choix d'algorithmes de chiffrement inappropriés

Mauvaise configuration

- Mots de passe par défaut
- Droits d'accès trop larges
- Mode debug actif dans une application
- Configuration incorrecte : panne Facebook du 4 octobre 2021 (analyse technique détaillée)

Bug - Exemple : Manipulation de chaînes de caractères en C

Problème numéro un : débordement de buffer

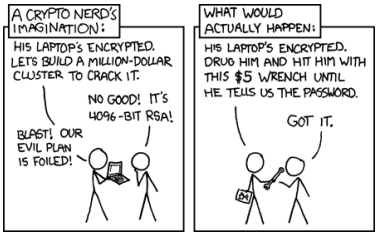
```
char path[128];

strcpy(path, getenv("$HOME"));
```

Si `$HOME` est trop longue :

- écrit en dehors de la variable `path` et écrase l'adresse de retour sur la pile.
- permet d'exécuter du code passé dans `$HOME`.

Facteur humain

- Ingénierie sociale
  - Phishing https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage
  - Arnaque au président : https://www.economie.gouv.fr/dgccrf/larnaque-au-president-toujours-tres-frequente
- https://xkcd.com/538/



Environnement vulnérable

- Internet
- Cloud
- IoT (le S veut dire sécurité)

Histoire

- Reflections on Trusting Trust par Ken Thompson. Cheval de Troie dans le compilateur ? (1984)
- Stoned Premiers Virus via disquettes (1987)
- Vers Morris 1er vers internet (sendmail) (1988)
- Smashing the Stack for Fun and Profit exploitation du débordement de pile (1996)
- Smurf 1ers Dénis de service distribués (1998)
- Cryptolocker le 1er rançongiciel (2013) (Histoire)
- Meltdown et Spectre vulnérabilités matérielles sur la virtualisation (2017)
- Solar Winds attaques sur la supply chain (2020)

Menaces

Motivations :

- divertissement
- militantisme
- vengeance
- profit
- guerre / terrorisme

Avantages :

- Rapport bénéfices / risque plus élevé que dans d'autres domaines
- Relative facilité

Écosystème de la sécurité des systèmes d'information :

Coté attaque :

- marché des vulnérabilités 0 day
- acteurs étatiques (ou proches des états : APT xx, yyy Bear, NSO Group, ...)
- Groupes criminels (Mafias)

Coté défense :

- sociétés et chercheurs en sécurité (Google Project Zero, ZDI, DEFCON, CCC...)
- bug bounties des éditeurs
- CERT (US) et ANSSI (France)
- fournisseurs de solutions de sécurité (anti-virus, EDR, pare-feu, SOC, SIEM)

`https://homepages.laas.fr/matthieu/talks/campus-du-libre-21.pdf`

Risques

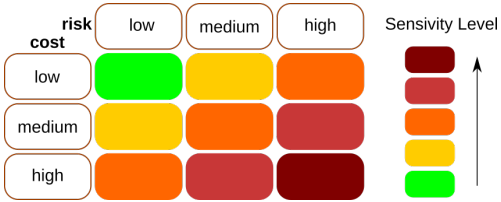
Résultante de l'existence de vulnérabilités et de menaces.

3 Types principaux par ordre de probabilité croissante (statistiques)

- **Accidentel :** panne matérielle, perte d'un appareil, destruction involontaire, dégât des eaux, incendie,...
- **Crime non ciblé :** vol ciblant uniquement la valeur de l'appareil
- **Crime ciblé :** vol ou attaque ciblant spécifiquement des données de la victime

Dommages et coûts

- Directs :
  - pertes financières : vol d'équipements, rançons,...
  - temps passé à restaurer les données / refaire les expériences
- Indirects :
  - divulgation de données sensibles
  - accès non-autorisés à d'autres systèmes
  - responsabilité civile (dommages et intérêts)
  - perte d'image / de crédibilité



Évaluer la sensibilité au regard des pertes potentielles en cas d'incident

Agenda

Incendie OVH - Disponibilité

- Dans la nuit du 9 au 10 mars 2021
- Destruction complète du Datacenter SBG-2 + partielle SBG-1
- Pas de sauvegardes explicitement prévues dans les contrats
- Perte totale d'un certain nombre de données

Rançongiciels

- Anatomie des attaques de rançongiciel récentes, un retour d'expérience (video)
- Récit Manutan février 2021
- État de la menace rançongiciel - ANSSI
- Attaque par rançongiciels tous concernés. Comment les anticiper et réagir en cas d'incident ? - ANSSI
- ENAC Toulouse (mars 2022), INP Toulouse (septembre 2022), INP Grenoble (décembre 2022)

Log4shell (décembre 2021)

- faille type 0 day
- (re)découverte par joueurs de Minecraft début décembre 2021
- bibliothèque log4j pour gérer les traces dans applications Java
- inclut un mécanisme d'évaluation de variables (et indirectement de code)
- nombreuses applications qui ne filtrent pas les chaînes en provenance des clients web avant de les passer à log4j
- $\rightarrow$ il est possible d'injecter du code java depuis un serveur externe (sous contrôle de l'attaquant)
- milliers de serveurs vulnérables
- exploitation active:
  - mineurs de crypto-monnaies
  - attaques plus ciblées pour rançongiciels
- Détails techniques

Agenda

Cadre légal

- Informatique et libertés (1978)
- Loi Godfrain (1998)
- LCEN (2004)
- DADSVI (2006)
- Hadopi (2009)
- Loppsi 2 (2011)
- Décrets PPST (2011)
- Loi Renseignement (2015)
- RGPD (2016)
- Pour une République numérique (2016)
- Transposition de la directive européene NIS (2018), puis NIS2 (2023)
- Sécurité Globale, Renseignement et lutte contre le terrorisme, 2021

Normes

- ISO 27xxx
  - Système de Management de la Sécurité de l'Information (SMSI) (27001)
  - Guides de bonnes pratiques (27002)
  - Analyse des risques (27005)
- Autres Méthodes /guides :
  - Mehari (Clusif),
  - EBIOS Risk Manager (ANSSI),...

Agenda

Recommandations générales

Règles de base pour la sécurité sur internet

1. bons mots de passe
2. systèmes et logiciels à jour
3. sauvegardes régulières
4. limiter l'utilisation de comptes privilégiés (administrateur)
5. prudence vis à vis des contenus
6. contrôler la diffusion des informations

Agenda

Cryptographie

Technologies de chiffrement de données.

- Confidentialité
- Intégrité
- Authenticité (signature numérique)

Principe de Kerckhoffs :

- la sécurité ne doit dépendre que du secret,
- les algorithmes utilisés doivent être publics

Types d'algorithmes

- symétrique : un secret partagé - AES, ChaCha20,...
- asymétrique : clé publique et clé privée - RSA, ED25519,...
- fonctions de hashage : calcul de condensats, - MD5, SHA1, SHA2,...

Mots de passe

Attaques par force brute (dictionnaires) ou phishing.

- au moins 12 caractères, la longueur est la meilleur protection.
- différentes classes de caractères (lettres, chiffres, symboles),
- pas de mots du dictionnaire, ni de variations simples
- **Ne pas réutiliser un mot de passe sur plusieurs systèmes**
- **Utiliser un mot de passe différent pour chaque site web.**
  - utiliser un gestionnaire de mot de passe.
  - ne pas stocker de mots de passe en clair dans son navigateur ou son téléphone utiliser un mot de passe maître et/ou un code PIN complexe
- Si un mot de passe est compromis :
  - changez-le partout où il était utilisé
  - informer les responsables du (des) site(s) où il était utilisés (opposition).

Authentification renforcée

Contre le phishing et les autres attaques par ingénierie sociale

- biométrie (empreintes digitales, reconnaissance faciale, iris, contour de la main,....)
- certificats électroniques / clés privées
- double facteur :
  - code de confirmation via SMS, email
  - mots de passe à usage unique (OTP) : applications sur téléphone ou boîtier dédié
  - Webauthn / FIDO2 : clé USB de sécurité

https://homepages.laas.fr/matthieu/talks/token-capitoul-2021.pdf

Chiffrement des données - Protection de la confidentialité

Plusieurs types :

En Transit sur les réseaux
HTTPS, SSH, messageries chiffrées,...
Chiffrement de bout en bout (E2EE) ou par un serveur central

FDE (Full Disk Encryption)
chiffrement de tout le disque. Protège contre perte/vol de la machine lorsqu'elle est éteinte ou en veille.
Lorsque la machine est en marche, toutes les données sont lisibles.

Container ou dossier chiffré
chiffrement d'un dossier dans une archive (style ZIP).
Déchiffrée uniquement lorsque nécessaire (accès au contenu).
Utile aussi pour le transfert de données (mail ou autre)

Sauvegardes

Protège des pertes accidentelles et des attaques (disponibilité).

- fréquentes (une fois par jour / en continu)
- sécurisées
  - site séparés
  - redondance
  - pas modifiables facilement
- testées (une sauvegarde pas testée n'existe pas !)

Techniques variées selon particulier ou entreprise / administration :

- synchronisation type cloud (Nextcloud, drive,...)
- logiciel dédié (gère les durées de conservation) ex: time machine Apple
- systèmes matériels dédiés (bandes magnétiques,...)

Mises à jour logicielles et outils de sécurité

- Appliquer les mises à jour de sécurité du système et des applications
- Installer et maintenir à jour un logiciel de sécurité (anti-virus + pare-feu)

En pratique : la majorité des attaques passent par des systèmes vulnérables pour lesquels le correctif existe mais n'est pas appliqué.

Vulnérabilité **0 day** : problème de sécurité pour lequel il n'y a pas de correctif connu.

https://homepages.laas.fr/matthieu/talks/siarsv2-protection-linux.pdf

Durcissement des systèmes

Rendre les bugs plus difficiles à exploiter

- pile système non exécutable
- langages de programmation « sûrs » (Ada, Rust,...)
- placement aléatoire des objets en mémoire
- génération automatique de code + vérification automatique
- protocoles et interfaces favorisant la sécurité
- limitation des privilèges
- ...

https://homepages.laas.fr/matthieu/cours/mh-prog-defensive.pdf

TLS et le chiffrement du trafic réseau

Certificats Numérique : preuve de l'identité du détenteur
Infrastructure de gestion des clés (confiance centralisée)
Base de la sécurité pour les applications Web et Cloud.

Connexions HTTPS :

- vérification de la validité du certificat du site
- négociation de paramètres de chiffrement et de contrôle de l'intégrité (algorithmes + clé éphémère)
- authentification optionnelle du client via son certificat
- sinon : login / mot de passe / authentification à 2 facteurs ,...

Versions actuelles: TLS 1.3, HTTP/3.0, QUIC 1.0

`https://homepages.laas.fr/matthieu/talks/siarsv2-chiffrement-services.pdf`

Prudence vis à vis des données externes

Toute donnée inconnue peut être malveillante. Par exemple :

- messages de phishing, et autre arnaques au président
- sites web infectés / code javascript malveillant / espionnage
- clé USB infectée abandonnée sur un parking, dans un lieu public,
- traceurs et espions dans les applications mobiles (cf exodus privacy)

Protection : limiter les privilèges (pas de compte admin),
cloisonner les applications (par exemple : Qubes OS)

`https://homepages.laas.fr/matthieu/talks/app-sec-article.pdf`

Sécurité dans le développement de projets informatiques

Créer une culture de la sécurité pour les systèmes d'information.

- Prendre en compte la sécurité dès la conception initiale
- Faire une analyse des risques
- Lien avec RGPD : conception pour la protection des données personnelles
- Faire auditer les choix par des experts
- Prévoir les mises à jour et les correctifs de sécurité
- Mettre en place un mécanisme pour signaler les problèmes de sécurité

Agenda

Principe d'une politique de sécurité

Définis dans ISO27001, calquée sur ISO 9000 (Qualité)

- Définir des objectifs de sécurité mesurables (indicateurs)
- Évaluer l'écart entre la réalité et les objectifs
- Agir sur le système pour réduire l'écart
- Itérer

Risques résiduels :

- accepter
- externaliser (sous-traitance, assurance,...)

Plans de continuité / reprise d'activité

Font partie de la politique de sécurité.

PCA Plan de Continuité de l'Activité
Comment assurer la disponibilité du service ?

PRA Plan de Reprise de l'Activité
Comment re-démarrer après un incident majeur ?

- Gestion de crise
- Soutien humain
- Redondance des infrastructures sur plusieurs sites
- Tests réguliers de basculement
- Protection contre le « split brain »

Exemple: la PSSIE

Politique de Sécurité des Systèmes d'Information de l'État (2014)
Définie par l'ANSSI.
https://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf
Ensemble d'une centaine de règles à appliquer dans toutes les administrations de l'État.

Agenda

Conclusion

Vaste domaine...

Nécessite une réflexion

- aspects techniques
- aspects organisationnels
- aspects juridiques et sociétaux

Questions ?

Agenda

Bibliographie

- **Cyber fragiles, enquête sur les dangers de nos vies connectées**, B. Mao et T. Saintourens, Éditions Taillandier, 2016, ISBN 979-10-210-1806-8
- **La face cachée d'internet**, R. Stamboliyska, Éditions Larousse, 2017, ISBN 978-2-03-593641-7
- **Fous de codes (secrets)**, M. Frary, Éditions Flammarion, 2017, ISBN 978-2-0813-9556-5
- **Histoire des codes secrets**, S. Singh, Éditions JC Lattès, 1999, ISBN 2-7096-2048-0

Sites et organismes de référence

- ANSSI Agence Nationale de la Sécurité des Systèmes d'Information
- ENISA European Union Agency for Cybersecurity
- Clusif Club de la Sécurité Informatique Française
- OSSIR Observatoire de la Sécurité des Systèmes d'Information
- Club 27001 Club des utilisateurs des normes ISO 2700x
- OWASP France Open Web Application Security Project

- No Limit Secu Podcast dédié à la cyber sécurité
- Technique et droit du numérique Blog en BD de Maître Marc-Antoine Ledieu, avocat spécialiste en droit des systèmes d'information.