Rapport de cours
Jour 2

Victoria SAUTEREAU

Cybersécurité

ESTIAM

École d'informatique
et du numérique

2ème année
2022/2023

Sommaire

Partie 1 : La cryptographie ?

Qu'est-ce la cryptographie

La cryptographie est une méthode permettant de stocker et de transmettre des données, de sorte que seul le destinataire désigné puisse les lire ou les traiter. La cryptographie moderne utilise des algorithmes sécurisés pour s'assurer que les cybercriminels ne puissent pas facilement compromettre des informations protégées.

La confidentialité des données garantit que seul le destinataire pourra lire le message. Pour ce faire, les deux parties ont recours au chiffrement. Il s'agit d'un processus qui consiste à brouiller les données afin de rendre leur lecture difficile par une partie non autorisée.

L'histoire de la cryptographie

La cryptographie a vu le jour dans les cercles diplomatiques il y a plusieurs milliers d'années. Les messagers de la cour d'un roi amenaient des messages cryptés à d'autres cours. Il arrivait que d'autres cours, qui n'étaient pas impliquées dans la communication, essayent de voler les messages envoyés à un royaume qu'ils considéraient comme leur adversaire. Peu de temps après, les chefs militaires ont commencé à utiliser le chiffrement pour protéger leurs messages.

Toutes les méthodes de chiffrement utilisent une clé pour chiffrer ou déchiffrer un message. Cette clé est une composante importante de l'algorithme de chiffrement. L'efficacité d'un algorithme de chiffrement dépend de la clé utilisée. Plus la clé est complexe, plus l'algorithme est sécurisé. La gestion des clés est un facteur essentiel du processus.

Les types de chiffrement

Il existe 2 types de chiffrement:

- Chiffrement par clé privée
- Chiffrement par clé publique

1. Chiffrement par clé privée

Les algorithmes symétriques utilisent la même clé prépartagée pour chiffrer et déchiffrer les données ; une méthode également connue sous le nom de chiffrement par clé privée. Le chiffrement par clé privée utilise un algorithme symétrique.

De nombreux systèmes de chiffrement utilisent une méthode symétrique. Voici certaines normes de chiffrement courantes basées sur une méthode symétrique:

3DES (Triple DES) : DES (Digital Encryption Standard) est un algorithme de chiffrement symétrique avec une taille de bloc de 64 bits qui utilise une clé de 56 bits. Il prend un bloc de texte en clair de 64 bits en entrée et génère un bloc de texte crypté de 64 bits. Il fonctionne toujours sur des blocs de taille identique, et utilise les méthodes

de permutation et de substitution dans l'algorithme. La permutation est une méthode d'organisation de tous les éléments d'un ensemble.

Triple DES chiffre les données trois fois et utilise une clé différente au moins une fois sur trois, d'où une taille de clé cumulée de 112 à 168 bits. L'algorithme 3DES résiste aux attaques, mais se montre beaucoup plus lent que DES.

Le cycle de chiffrement 3DES se présente comme suit:

1. Données chiffrées par le premier DES

2. Données déchiffrées par le deuxième DES

3. Données chiffrées à nouveau par le troisième DES

Le texte chiffré est déchiffré en suivant la procédure inverse.

IDEA : l'algorithme IDEA (International Data Encryption Algorithm) utilise des blocs de 64 bits et des clés de 128 bits. IDEA réalise huit sessions de transformations sur chacun des 16 blocs qui résultent de la division de chaque bloc de 64 bits. IDEA a remplacé DES ; PGP (Pretty Good Privacy) l'utilise dorénavant. PGP est un programme qui assure la confidentialité et l'authentification des communications de données. GnuPG ou GPG (GNU Privacy Guard) est une version gratuite de PGP distribuée sous licence.

AES : l'algorithme AES (Advanced Encryption Standard) a une taille de bloc fixe de 128 bits, avec une taille de clé de 128, 192 ou 256 bits. L'institut NIST (National Institute of Standards and Technology) a approuvé l'algorithme AES en décembre 2001. Le gouvernement américain utilise AES pour protéger les informations classifiées.

AES est un puissant algorithme qui utilise des clés plus longues. Plus rapide que DES et 3DES, il constitue une solution adaptée aussi bien aux applications logicielles qu'au matériel utilisé dans les pare-feu et les routeurs.

Skipjack (développé par la NSA), Blowfish et Twofish sont d'autres types de chiffrement par bloc.

2. Chiffrement par clé publique

Le chiffrement asymétrique, appelé également chiffrement à clé publique, utilise une clé pour le chiffrement et une autre pour le déchiffrement. Il est impossible pour un criminel de calculer la clé de déchiffrement d'après la clé de chiffrement et inversement dans un délai raisonnable.

Les algorithmes asymétriques utilisent des formules que tout le monde peut consulter. L'utilisation d'une paire de clés non liées constitue un gage de sécurité. Voici les algorithmes asymétriques:

RSA (Rivest-Shamir-Adleman) : cet algorithme utilise le produit de deux très grands nombres premiers de même longueur, entre 100 et 200 chiffres. Les navigateurs utilisent RSA pour établir une connexion sécurisée.

Diffie-Hellman : fournit une méthode d'échange électronique pour partager la clé secrète. Les protocoles sécurisés comme SSL (Secure Sockets Layer), TLS (Transport Layer Security), SSH (Secure Shell) et IPsec (Internet Protocol Security) utilisent Diffie-Hellman.

ElGamal: utilise le standard du gouvernement des États-Unis pour les signatures numériques. Cet algorithme n'étant protégé par aucun brevet, il peut être utilisé gratuitement.

Cryptographie sur les courbes elliptiques (ECC): utilise des courbes elliptiques pour créer un algorithme. Aux États-Unis, la NSA (National Security Agency) utilise ECC pour générer des signatures numériques et échanger des clés.

Conclusion: Il est important de connaître les différences entre les méthodes de chiffrement asymétrique et symétrique. Les systèmes de chiffrement symétrique sont plus efficaces et gèrent un plus grand nombre de données. Cependant, la gestion des clés est plus problématique et plus complexe. La cryptographie asymétrique protège plus efficacement la confidentialité de petits volumes de données. De plus, vu sa taille et sa vitesse, elle sécurise mieux certaines tâches, comme l'échange de clés électroniques qui implique de faibles volumes de données au lieu de chiffrer d'importants blocs de données.

Partie 2 : Les contrôles d'accès

- ## Types d'accès

1. Contrôle d'accès physiques

Les contrôles d'accès physiques sont les barrières mises en place pour empêcher tout contact direct avec les systèmes. L'objectif est d'empêcher des utilisateurs non autorisés d'accéder physiquement aux sites, aux équipements et aux autres ressources de l'entreprise. Le contrôle d'accès physique détermine quels individus sont autorisés à entrer (ou sortir), où et quand ils peuvent entrer (ou sortir).

2. Contrôle d'accès logiques

Les contrôles d'accès logiques désignent les solutions matérielles et logicielles utilisées pour gérer l'accès aux ressources et aux systèmes. Ces solutions technologiques englobent des outils et des protocoles utilisés par les systèmes informatiques pour l'identification, l'authentification, l'autorisation et la responsabilisation.

Voici quelques exemples de contrôles d'accès logiques:

- Le chiffrement est un processus qui consiste à convertir du texte en clair en texte crypté.
- Les cartes à puce disposent d'une micropuce intégrée.
- Un mot de passe est une chaîne de caractères protégée.
- La biométrie analyse les caractéristiques physiques d'un utilisateur.
- Les listes de contrôle d'accès (ACL) définissent le type de trafic autorisé sur un réseau.
- Les protocoles sont des ensembles de règles qui régissent l'échange de données entre des appareils
- Les pare-feu bloquent le trafic indésirable.
- Les routeurs connectent au moins deux réseaux.
- Les systèmes de détection d'intrusion (IDS) surveillent les activités suspectes sur un réseau.
- Les niveaux de coupure définissent des seuils d'erreurs autorisés avant le déclenchement d'une alerte.

3. Contrôle d'accès administratifs

Les contrôles d'accès administratifs sont des politiques et des procédures mises en place par les entreprises pour contrôler les accès non autorisés. Les contrôles administratifs se concentrent sur les pratiques personnelles et professionnelles. Voici quelques exemples de contrôles d'accès administratifs:

- Les politiques sont des déclarations d'intention.
- Les procédures détaillent les étapes à suivre pour effectuer une activité.
- Les pratiques de recrutement décrivent les procédures suivies par une entreprise pour trouver des employés qualifiés.
- La vérification des antécédents est un processus de filtrage des employés qui porte sur les antécédents professionnels, l'historique de crédit et les antécédents criminels d'un candidat.
- La classification des données classe les données en fonction de leur niveau de sensibilité.
- Une formation à la sécurité sensibilise les employés aux politiques de sécurité en vigueur dans l'entreprise.
- Une évaluation permet de mesurer le rendement d'un employé.

Identification

L'identification applique les règles établies par la politique d'autorisation. Un sujet demande à accéder à une ressource du système. À chaque fois que le sujet demande à accéder à une ressource, les contrôles d'accès déterminent s'il convient de lui autoriser ou de lui interdire l'accès à cette ressource. La police d'autorisation détermine, par exemple, les opérations qu'un utilisateur peut effectuer sur une ressource.

Un identifiant unique garantit une association correcte entre les opérations autorisées et les sujets. Le nom d'utilisateur est la méthode utilisée le plus couramment pour identifier un utilisateur. Il peut s'agir d'une combinaison de caractères alphanumériques, d'un code PIN, d'une carte à puce ou d'une caractéristique biométrique, telle qu'une empreinte digitale, une lecture rétinienne ou la reconnaissance vocale.

Un identifiant unique permet à un système d'identifier chaque utilisateur individuellement, c'est-à-dire de donner la permission à un utilisateur autorisé d'effectuer des actions appropriées sur une ressource donnée.

- ## Autorisation

L'autorisation détermine ce qu'un utilisateur peut faire et ne pas faire sur un réseau après s'être authentifié. Dès qu'un utilisateur a prouvé son identité, le système vérifie les ressources réseau auxquelles il peut accéder et les opérations qu'il est autorisé à effectuer. Comme le montre cette illustration, l'autorisation répond à la question suivante : « Quels privilèges de lecture, de copie, de création et de suppression l'utilisateur possède-t-il ? »

L'autorisation utilise un ensemble d'attributs qui décrivent l'accès de l'utilisateur au réseau. Le système compare ces attributs aux informations enregistrées dans la base de données d'authentification, détermine un jeu de restrictions applicables à cet utilisateur et le transmet au routeur local auquel l'utilisateur est connecté.

L'autorisation est un processus automatique qui ne requiert, de la part des utilisateurs, aucune étape supplémentaire après l'authentification. Implémentez l'autorisation immédiatement après l'authentification de l'utilisateur.

- ## Traçabilité

La traçabilité permet de remonter à la source d'une action et d'identifier ainsi la personne ou le processus qui a apporté une modification à un système. Cette opération collecte ensuite ces informations et génère un rapport sur les données d'utilisation.

L'entreprise peut utiliser ces données à diverses fins, comme les audits ou la facturation. Parmi les données collectées, on trouve l'heure de connexion d'un utilisateur, si l'utilisateur a réussi à se connecter ou non, ou les ressources réseau que l'utilisateur a consultées.

L'entreprise peut ainsi assurer le suivi des actions et des erreurs survenues lors d'un audit ou d'une enquête.

- ## Authentification

L'authentification est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).

Partie 3 : Dissimulation des données

- ## Masquage des données

1. En quoi consiste le masquage de données

La technologie de masquage de données sécurise les données en remplaçant les informations sensibles par une version non sensible. La version non sensible ressemble à l'original. Un processus métier peut donc utiliser des données non sensibles sans avoir à modifier les applications qui les prennent en charge, ni les sites de stockage des données. Dans la plupart des cas, la dissimulation limite la propagation des données sensibles dans les systèmes IT en utilisant des données de substitution à des fins de test et d'analyse. Le masquage des données peut s'opérer de manière dynamique si le système ou l'application détermine qu'une demande d'informations sensibles introduite par l'utilisateur est risquée.

2. Techniques de masquage de données

Le masquage de données peut remplacer des données sensibles dans les environnements hors production afin de protéger les informations sous-jacentes.
Plusieurs techniques de masquage de données permettent de faire en sorte que les données restent compréhensibles, tout en les modifiant suffisamment pour les protéger. La substitution remplace les données par des valeurs authentiques en apparence afin de rendre anonymes les enregistrements de données. Le brassage déduit un ensemble de remplacement de la même colonne de données que celle qu'un utilisateur souhaite masquer. Cette technique convient parfaitement aux données financières dans une base de données test, par exemple. La technique d'annulation applique une valeur nulle à un champ donné, ce qui empêche toute visibilité des données.

- ## Sténaganographie

1. Qu'est-ce que la stéganographie ?

La stéganographie dissimule les données (le message) dans un autre fichier, comme un graphique, un fichier audio ou un autre fichier texte. La stéganographie présente un avantage par rapport à la cryptographie : le message secret n'attire pas spécialement l'attention.

2. Les techniques de stéganographie ?

La méthode du bit de poids faible (LSB) est utilisée pour intégrer les données dans une image de couverture. Cette méthode utilise des bits de chaque pixel de l'image. Le pixel est l'unité de base d'une couleur programmable dans une image informatique. La couleur exacte d'un pixel est une combinaison de trois couleurs : le rouge, le vert et le bleu (RVB). Trois octets de données définissent la couleur d'un pixel (un octet par couleur). Huit bits forment un octet. Un système couleur 24 bits utilise les trois octets.

La méthode LSB utilise un bit de chacune des composantes couleur rouge, verte et bleue. Chaque pixel peut stocker trois bits.

3. La stéganographie sociale

Le stéganographie sociale consiste à dissimuler des informations en créant un message lisible d'une certaine manière par une certaine audience. Le message n'est pas compréhensible par les autres personnes qui lisent les informations « normalement ». Les adolescents actifs sur les réseaux sociaux utilisent cette technique pour circonscrire certaines informations à un cercle social spécifique (leurs plus proches amis, par exemple), en s'assurant qu'elles ne sortent pas du contexte de ces relations. Par exemple, l'expression « aller au cinéma » peut signifier « aller à la plage ».

La stéganographie sociale est également utilisée dans les pays qui censurent les médias. Pour faire passer un message, les utilisateurs peuvent faire volontairement des fautes d'orthographe ou utiliser des références obscures. En réalité, ils communiquent simultanément avec différentes audiences.

4. Détection

La stéganalyse a pour vocation de détecter si un élément est susceptible de contenir des informations cachées et de révéler ensuite ces informations.
Les motifs de l'image stéganographique paraissent suspects. Un disque peut, par exemple, contenir des zones inutilisées où sont dissimulées des informations. Les utilitaires d'analyse de disque peuvent signaler les informations cachées dans les clusters inutilisés des supports de stockage. Les filtres peuvent capturer des paquets de données dont les en-têtes contiennent des informations cachées. Ces deux méthodes utilisent des signatures de stéganographie.
En comparant l'image d'origine à l'image stéganographique, un analyste peut relever visuellement des schémas répétitifs.

• Obfuscation des données

1. Obfuscation

L'obscurcissement de données est l'utilisation et la pratique des techniques de stéganographie et de masquage de données dans le domaine de la cybersécurité. L'obfuscation consiste à rendre le message confus, ambigu ou difficile à comprendre. Un système peut intentionnellement brouiller les messages pour éviter tout accès non autorisé à des informations sensibles.

2. Application

Le filigrane logiciel protège les logiciels contre tout accès non autorisé ou toute modification. Le filigrane logiciel insère un message secret dans le programme comme preuve de propriété. Ce message secret correspond au filigrane logiciel. Si quelqu'un tente de supprimer le filigrane, le code ne fonctionnera plus. L'obscurcissement logiciel convertit un logiciel en une version équivalant à l'original, mais plus difficile à analyser pour les agresseurs. Toute tentative de rétro-ingénierie du logiciel donnera des résultats incompréhensibles à partir du logiciel qui continue de fonctionner.