Rapport 2 : Ingénierie Crypto

Membres du groupe :

- *Papa Abdou CALLOGA*
- *Yacine DIAGNE*
- *Yaye Khadidiatou DIOP*
- *Aby NDIAYE*
- *Alioune SALL*

Professeur : *M. MENDY*

Table des matières

Introduction

Le cryptologue élabore des méthodes et mécanismes de codage à partir d'algorithmes élaborés et complexes pour protéger toutes les données sensibles (mots de passe, identifiants de compte en banque, numéro de cartes bancaires), assurer la confidentialité des transmissions et garantir l'authenticité et l'intégrité des données. Le choix de notre sujet est alors totalement en lien avec le contenu du cours car traitant des défaillances qui peuvent exister dans les différents algorithmes qu'elle soit classique , à clé sécurisée ou publique .

Le traitement de ce sujet nous permettra alors de mettre en pratique les différentes notions abordées dans ce cours .

Cette vulnérabilité a un lien central avec le cours, dans lequel on aborde les types d'algorithmes cryptographiques, leur fiabilité selon des critères divers.

Méthodologie de travail

- Choix d'une catégorie de vulnérabilité parmi le Top 10 de Owasp
- Matching avec les concepts présents dans les différents chapitres du cours
- Analyse des scénarios (démos, propositions et outils utilisés)
- Ajouter des scénarios
- scénarios de défense
- Cryptanalyse

Lien entre la A02 : Défaillances cryptographiques et le cours

1. Chapitre 3 : Cryptographie classique

Dans ce chapitre, on parle de la cryptographie classique qui regroupe l'ensemble des techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible.
Elle fait intervenir la notion de chiffrement qui consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.
Différentes techniques de chiffrement ont été abordées dans le cours en passant par le chiffrement à substitution jusqu'au chiffrement par transposition.
Le premier type de chiffrement consiste à remplacer les symboles d'un texte en clair par d'autres symboles sans en bouleverser l'ordre. A cet effet, le chiffrement de César en est une parfaite illustration, il consiste simplement à décaler les lettres de l'alphabet d'un nombre de positions constant vers la droite ou la gauche.
Par exemple, avec un décalage vers la gauche de 3, D est remplacé par A, E devient B, et ainsi de suite.
Cet algorithme de chiffrement est naturellement simple donc facilement déchiffrable. Par conséquent, c'est un algorithme de chiffrement faible. Pour casser le code de César il suffit de tester autant de décalages possibles qu'il n'y a de lettres dans l'alphabet.
Si lors de l'envoi d'un message, le technique du chiffrement de César est utilisée, deux situations peuvent être envisagées :

- Un attaquant sait (ou devine) qu'une sorte de chiffrement de substitution simple a été utilisé, mais pas spécifiquement le chiffrement de César
- Un attaquant sait qu'un chiffrement de César est utilisé mais ne connaît pas la valeur de décalage.

Dans le premier cas, le chiffrement peut-être cassé en utilisant les mêmes techniques que pour un chiffrement par substitution simple général, comme l'analyse de fréquence (notion abordée dans le cours)

Rappel : L'analyse de fréquences ou analyse fréquentielle est une

méthode de cryptanalyse. Elle consiste à examiner la fréquence des lettres employées dans un message chiffré. Cette méthode est fréquemment utilisée pour décoder des messages chiffrés par substitution (comme par exemple le Chiffre de Vigenère ou le Chiffre de César).
Dans le second cas, casser le schéma est encore plus simple. Comme il n'y a qu'un nombre limité de décalages possibles (25 en anglais), ils peuvent chacun être testés à tour de rôle dans une attaque par force brute qu i consiste de manière générale ..... (définition).

Dans tous les deux cas, on remarque de nettes défaillances cryptographiques. Car un utilisateur hors système est capable de déchiffrer un message qui ne devait être compréhensible que par un destinataire spécifique.
Il est cependant utile de noter que l'inconvénient majeur des techniques de chiffrement à substitution simple est l'analyse de fréquence. Pour corriger cela, on a mis en œuvre le polyalphabétisme. Ce type de chiffrement est basé sur la substitution , utilisant plusieurs alphabets de substitution. Le chiffre de Vigenère est probablement l'exemple le plus connu de chiffre polyalphabétique. C'est une amélioration du chiffrement de César, il repose sur une clef de chiffrement se présentant sous forme de mot ou de phrase permettant de chiffrer de manières différentes le même mot ou la même phrase en fonction de la clé.

2. Chapitre 4: Cryptographie à clé secrète

Ce chapitre porte sur la définition, les concepts et les formes de cryptographie à clé secrète.

Celle-ci, aussi dite « cryptographie symétrique », fait partie des trois types de chiffrement possibles, et permet à la fois de chiffrer et de déchiffrer des messages, à l'aide d'un même mot clé.

Ce chapitre est donc d'emblée en rapport avec A02 : Défaillances cryptographiques, puisqu'il s'agit de s'intéresser à des méthodes de cryptages et bonnes pratiques permettant d'éviter des vulnérabilités de cette catégorie.

Pour mieux faire ressortir le rapport entre ce chapitre et la catégorie A02, nous allons nous intéresser à quelques points, jugés pertinent à notre

approche, et tirés directement de l'OWASP (https://owasp.org/Top10/fr/A02_2021-Cryptographic_Failures/)

- Les algorithmes utilisés sont faibles ou désuets ;

Les algorithmes de chiffrement par clé secrète sont connus et largement utilisés pour garantir la confidentialité et l'intégrité des données.

Cependant, certains de ces algorithmes sont cassables et donc leur utilisation introduit une vulnérabilité certaine dans nos systèmes. Un des algorithmes de chiffrement symétrique, réputé pour sa vulnérabilité aux attaques est celui de César.

- Des clefs de chiffrement faibles sont générées ou utilisées :

Les algorithmes de chiffrement symétrique sont d'emblée moins sécurisés, dû au fait que la clé secrète est facilement transmissible. Il est d'ailleurs recommandé de les utiliser spécifiquement dans des situations où on est train de chiffrer un mot de passe que l'on souhaite réutiliser.

(cf https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/#:~:text=Sym%C3%A9trique%20par%20le%20fait%20d,le%20chiffrement%20et%20le%20d%C3%A9chiffrement.&text=Asym%C3%A9trique%20par%20le%20fait%20d,le%20m%C3%AAme%20algorithme%20de%20chiffrement)

Cependant, même dans ces situations, si les clefs générées sont faibles, ou réutilises (comme dans le mode ECB du cryptage par bloc), cela introduit une vulnérabilité.

- Les vecteurs d'initialisation sont ignorés, réutilisés ou générés avec une sécurité insuffisante pour le mode d'opération cryptographique

Par exemple, dans le mode CBC du chiffrement par bloc, des blocs de texte chiffrés identiques sont obtenus lorsque le même texte en clair est chiffré

sous la même clé et le vecteur v. Ce vecteur d'initialisation n'a pas besoin d'être chiffré, mais ne doit pas être utilisé avec la même clé.

Ce point est renforcé par OWASP, qui le cite comme un facteur nous rapprochant des vulnérabilité de la categorie A02.

- Des méthodes cryptographiques de remplissage dépréciées, comme PKCS 1 v1.5 sont utilisées

En cryptographie, le remplissage ou bourrage (padding) consiste à faire en sorte que la taille des données soit compatible avec les algorithmes utilisés. Un grand nombre de schémas cryptographiques décrivent des algorithmes qui utilisent un partitionnement en blocs de taille fixe. Si la taille des données n'est pas un multiple de la taille d'un bloc alors l'utilisation d'un schéma de remplissage doit être envisagé.

Cette notion de remplissage apparait dans les deux types de cryptage abordés dans le chapitre 4 :

chiffrement par bloc : le remplissage permet d'avoir un bloc de la taille adéquate si celui-ci est trop court (par exemple en ajoutant des 0) ;

chiffrement par flot : le remplissage peut éviter d'avoir une longueur par flot susceptible d'être attaquée, cela évite aussi que l'attaquant ne connaisse la taille du flux ;

3. Chapitre 5 : Cryptographie à clé publique

Dans ce chapitre on traite du problème de la cryptographie a clé publique qui consiste a partagé sa clé publique qui permet par la suite de déchiffrer le message puis de garder secrète sa clé privée avec laquelle on chiffre le

message .

En cas pratique on a parlé d'algorithmes de chiffrement tres celebre tel que RSA , Rabin ,ELGama.

Dans le cas de l'algorithme de RSA nous avons traité deux de ses attaques a savoir :

- Attaque à texte chiffré choisi
- Attaque par module commun

Ces deux attaques faisant montre de la défaillance cryptographiques de RSA ce qui rentre en plein dans le sujet que nous avons choisi qui s'intitule défaillances cryptographiques .

Pour plus étayer nos propos quant au rapport non contesté de notre sujet avec ce chapitre spécifique nous allons nous appuyer sur l'article de roca parlant des vulnérabilités qui menacent les clé de nombreux appareils. (https://www.lemagit.fr/actualites/450428952/ROCA-la-vulnerabilite-qui-menace-les-cles-de-nombreux-appareils)

Dans cet article, on apprend malheureusement que des chercheurs ont réussi à lever le voile sur une faille dans l'implémentation de l'algo de chiffrement RSA ce qui peut permettre à des attaquants de dérober les clés secrètes d'appareils vulnérables .

Cette vulnérabilité est caractérisée par une structure spécifique des nombres premiers générés , rendant possible la factorisation des clés de longueur courante , y compris sur 1021 et 2048 bits .

Dès lors, la seule connaissance d'une clé publique est nécessaire.Donc il n'y aucun doute de la corrélation qui existe entre notre sujet avec le chapitre 5 du cours d'ingénierie cryptographique .

4. Chapitre 6 : Fonctions de hachage

Ce chapitre traite des fonctions de hachage. Il est divisé en 3 étapes :

- Notions de fonctions de hachages cryptographiques
- Classifications et propriétés de ces fonctions
- Conceptions des fonctions de hachages

Une fonction de hachage est une fonction qui prend en entrée une donnée initiale pour calculer une sortie appelée empreinte numérique permettant d'identifier rapidement la donnée initiale.

La différence entre les fonctions de hachage et celle cryptographique est que la dernière est à sens unique. C'est a dire a partir de l'image il est difficile de retrouver l'antécédent a partir de la fonction de hachage.

- Résistance à la collision → une fonction de hachage crypto dont le calcul de la préimage est de complexité : O(2^N)

C'est à dire quand un attaquant dispose l'empreinte numérique la probabilité de retrouver la donnée initiale est 2^n : la propriété de résistance à la collision

- Application de la fhc: intégrité et authentification des messages
- Les algorithmes macs sont des fonctions de hachages qui prennent en entrées : le message et la clé du coup impossible de produire la même sortie sans connaissance de la clé
- Intégrité des données : La valeur de hachage d'un message x est calculée puis protégée a un instant T1 , a un instant T2 la valeur de hachage du message x' est calculée. Pour vérifier l'intégrité du message x a T2 on compare les valeur de hachage x et x' s'ils sont égales, on accepte que le message n'a pas été modifié.
- L'association entre une donnée initiale devrait être de telle sorte qu'une donnée initiale est identifiée de façon unique avec sa valeur de hachage avec une probabilité quasi inexistante de collision (les fonctions de hachages sont non injectives).
- Le système de crypto-monnaie s'appuie sur des mécanismes de cryptographie simples tels que les hachages cryptographiques et les signatures numériques.

Il existe deux types de fonctions de hachages cryptographiques :

- fhc sans clé
- fhc avec clé

Deux propriétés des fhc :

- compression → entrée de nb bits arbitraire / sortie de n bit fixe
- facilité de calcul de h(x) a partir de x
- Parmi les fonctions de hachages sans clé on distingue deux types :

  WHF → difficulté de trouver une entrée à partir d'une valeur de hachage pre-spécifiée.

  CRHF → résistance à la collision cad il est difficile de trouver deux valeur d'entrée ayant la mm valeur de hachage

- Fonction de hachages avec clé : Macs

En effet la vulnérabilité A02 du top 10 owasp est axée sur l'exposition des données sensibles. On pourrait voir le lien de cette vulnérabilité avec le chapitre 6 traitant les fonctions de hachages cryptographiques qui est un moyen de chiffrement des message par reconnaissance de ce dernier a partir d'une empreinte numérique.

On pourrait repérer sur le description de la vulnérabilité l'éventualité suivante :

Des fonctions de hachage dépréciées telles que MD5 ou SHA1 sont utilisées ou est-ce que des fonctions de hachage non cryptographiques sont utilisées là où des fonctions de hachage cryptographiques sont nécessaires.

Bibliographie/Webographie

1. https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/

2. https://www.synetis.com/notion-de-cryptologie-et-algorithme-de-chiffrement/#:~:text=Sym%C3%A9trique%20par%20le%20fait%20d,le%20chiffrement%20et%20le%20d%C3%A9chiffrement.&text=Asym%C3%A9trique%20par%20le%20fait%20d,le%20m%C3%AAme%20algorithme%20de%20chiffrement

3. https://owasp.org/Top10/fr/A02_2021-Cryptographic_Failures/

4. https://www.lemagit.fr/actualites/450428952/ROCA-la-vulnerabilite-qui-menace-les-cles-de-nombreux-appareils