Publication limitée pour le Conservatoire National des Arts et Métiers et Orange Campus Cyber

2

CYBERDEF 101

Gouvernance InfoSec

ERIC DUPUIS

2023

Téléchargez une version à jour

Edition extraits cours étudiants Cnam

Edition du 12 mai 2023 pour la deuxième EDITION, Publication limitée pour le Conservatoire National des Arts et Métiers et Orange Campus Cyber, réalisé sous LaTeX(MacTex) avec Texifier

Merci à Véronique Legrand, titulaire de la chaire de Cybersécurité du CNAM et Eric Bornette de la Délégation Général pour l'Armement sans qui cette aventure d'un cours introductif à la cyberdéfense d'entreprise n'aurait pu démarrer.
Un grand merci aussi à nos auditeurs du Conservatoire de National des Arts et Métiers (CNAM) pour leur participation active à ce cours SEC101 grâce à qui cette compilation des notes d'enseignement a pu voir le jour, avec une mention spéciale aux contributeurs.

Contributions

(2019-2020) **David BATANY** - Cnam SEC101 : *Architecture et fonctionnement des Botnets*

(2020) **Céline JUBY** - Orange Cyberdefense : *Contributions d'amélioration et relectures*

Table des matières

INFOSEC SEC101

1 Politiques et architectures de sécurité

1.1 Gouvernance de la sécurité

Du risque aux implémentations de sécurité avec des composants de sécurité configurés, pilotés, et controlés.

1.1.1 Politique de sécurité

Une politique de sécurité est un ensemble de règles et de procédures destinées à protéger les actifs (matériels, logiciels, informations) d'une entreprise ou d'une organisation contre les menaces internes et externes. Elle définit les responsabilités et les autorisations en matière de sécurité, les moyens de prévention et de détection des incidents de sécurité, ainsi que les mesures à prendre en cas de violation de la sécurité.

Elle peut couvrir différents domaines, tels que la sécurité physique (accès aux locaux, utilisation des clés, protection contre les intrusions), la sécurité informatique (mot de passe, pare-feu, antivirus), la sécurité des données (sauvegarde, chiffre-

ment), la sécurité des communications (confidentialité, intégrité), la sécurité des processus (gestion des droits d'accès, respect de la vie privée).

Une politique de sécurité adaptée est nécessaire afin de protéger au juste besoin les actifs de l'entreprise contre les menaces externes et internes, telles que les cyberattaques, les fuites de données, les actes de sabotage, etc. Une politique de sécurité efficace se doit d'être régulièrement mise à jour et adaptée aux évolutions de l'environnement de l'entreprise et des menaces pesant sur elle. Elle doit donc être non seulement être tournée sur les enjeux internes mais ne doit pas oublier de deployer ses moyens de perception sur les menaces potentielles avec des activités d'intelligence économique et stratégique.

1.2 Architectures de sécurité

Disposer des composants de sécurité dans une architecture de système d'information ne suffit pas totalement a assurer la sécurité de celui. Il est par ailleurs bien connus que la résistance d'un système, n'est pas directement liés à l'augmentation des systèmes de sécurité. Il est nécessaire de concevoir la « résistance et la résilience » du système des sa conception

1.2.1 Systèmes Cryptographiques

chapitre en cours de rédaction, DRAFT non publiable

1.2.2 Filtrages

Par signatures

chapitre en cours de rédaction, DRAFT non publiable

Par règles

chapitre en cours de rédaction, DRAFT non publiable

1.2.3 DMZ

chapitre en cours de rédaction, DRAFT non publiable

1.3 Sécurité des systèmes

Construire des systèmes dits surs nécessite de travailler sur deux plans :

- Rendre plus résistants les composants mêmes des systèmes d'information ou de l'environnement digital : on parle en particulier de *Security by Design*
- Ajouter des composants dont la fonction ajoute des mécanismes de protections.

1.3.1 Fonctions de sécurité

Les fonctions de sécurité de protection sont généralement construites pour protéger les grandes fonctions des systèmes d'information :

- Stocker : chiffrement, sauvegarde ... ;
- Traiter : redondance... ;
- Transporter : chiffrement, filtrage, isolation...

On peut aussi disposer de fonctions de sécurité dont la mission n'est pas de protéger au sens stricte du terme, mais apporter des fonctions de détection comme des IPS, IDS, SIEM, Honeypots.

Firewall Réseau : chapitre en cours de rédaction, DRAFT non publiable

Web Application Firewall : chapitre en cours de rédaction, DRAFT non publiable

IGC/PKI : chapitre en cours de rédaction, DRAFT non publiable

Coffre fort électronique : chapitre en cours de rédaction, DRAFT non publiable

DMZ : chapitre en cours de rédaction, DRAFT non publiable

Annuaire : Au coeur des systèmes d'authentification des entreprises

chapitre en cours de rédaction, DRAFT non publiable

VPN : chapitre en cours de rédaction, DRAFT non publiable

Signature : chapitre en cours de rédaction, DRAFT non publiable

Clés/token : chapitre en cours de rédaction, DRAFT non publiable

Proxy : chapitre en cours de rédaction, DRAFT non publiable

Routeur : chapitre en cours de rédaction, DRAFT non publiable

IPS/IDS : chapitre en cours de rédaction, DRAFT non publiable

1.3.2 Sécurité par construction

La notion de sécurité « par construction » est une notion large quand on parle de composants ou de système numérique. Le principe est d'introduire dès la conception des fonctions de sécurité sur la base des risques et des critères de menaces de l'environnement. (en n'oubliant pas les critères économiques).

Par ailleurs des mécanismes « d'autodéfense » et des mécanismes de notifications d'alertes (pouvant être des logs par exemple) peuvent être ajouté.

Le déploiement de ce concept au sein des projets se révèle un peu différents en fonction de la cible :

- **Sécurité d'un système d'information** : Dans la majorité des cas, l'entreprise possède des systèmes ayant déjà un certain degré de maturité. Les nouveaux projets s'intégrant dans le système d'information, nécessite un gouvernance plus complexe, et parler de Sécurité Intégrée et de conformité aux règles sécurité de l'entreprise. (intégration avec les services de sécurité

existant, utilisation de la PKI, des services de chiffrement, coffre fort, d'authentification)

- **Sécurité d'un produit** : (en n'oubliant pas les produits de sécurité qui eux même nécessitent une prise en compte des propriété de sécurité)
- **Sécurité d'un projet** ou système intégrant des composants informatiques

1.4 Défense en profondeur

chapitre en cours de rédaction, DRAFT non publiable

chapitre à compléter, les éléments ne donnent qu'une vue trop réduite ou parcellaire du sujet

1.5 les 4 critères de la sécurité

- la confidentialité des données informatiques
- l'intégrité des données
- la disponibilité des données informatiques
- l'authentification et la non-répudiation

1.6 Politiques de sécurité

chapitre en cours de rédaction, DRAFT non publiable

1.7 Gouvernance de la sécurité

chapitre en cours de rédaction, DRAFT non publiable

1.7.1 Système de management de la sécurité

chapitre en cours de rédaction, DRAFT non publiable

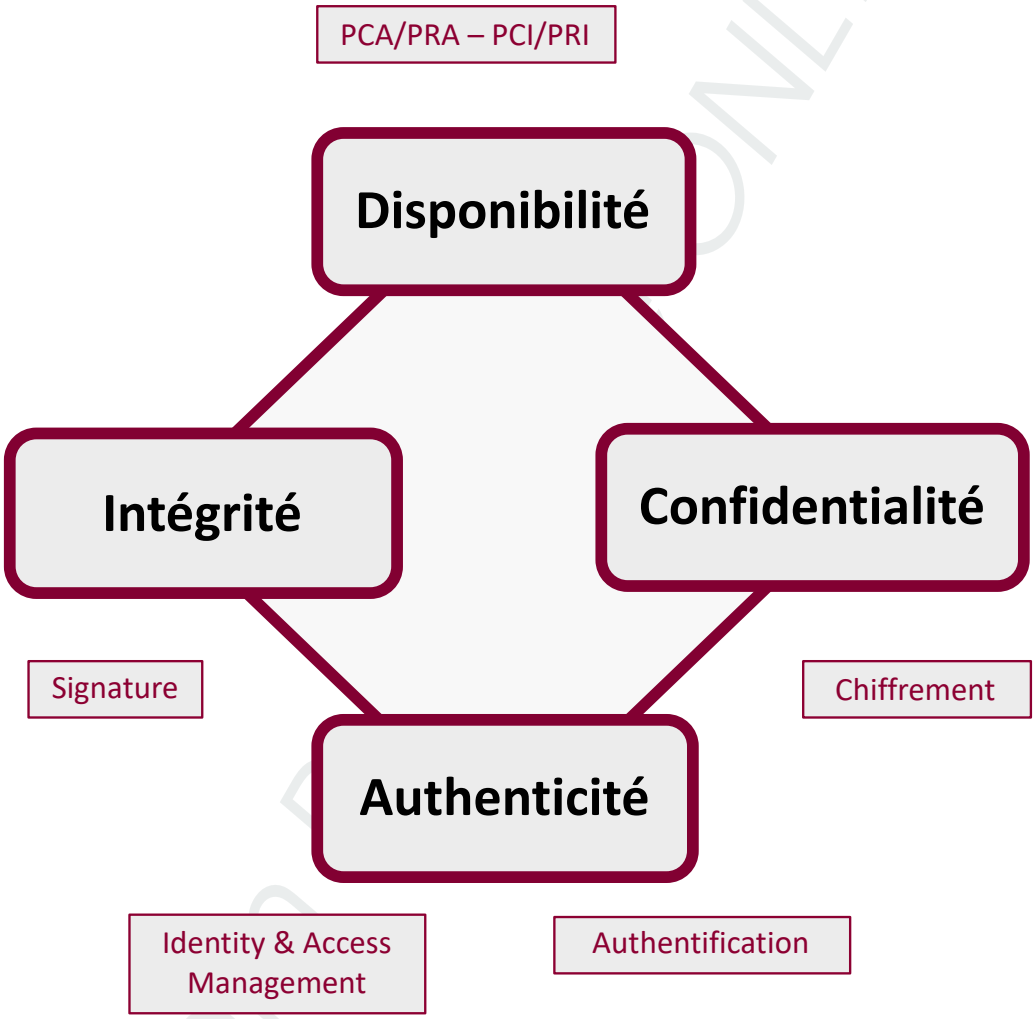

FIGURE 1.1 – (s) 4 critères fondamentaux

1.8 l'assurance de la sécurité

Grace aux outils d'analyse de risque, nous avons pu définir les biens essentiels de l'entreprise vu sous différents aspects :

- Continuité d'activité ;
- Protection du patrimoine informationnel et des données personnels ;
- Protection de l'image et de la réputation ;

Globalement, ces critères définissent le niveau de confiance que peuvent avoir les clients, et les partenaires dans l'entreprise.

La gouvernance de la sécurité, est un ensemble de responsabilités et de processus permettant de maintenir au quotidien le niveau de sécurité d'une organisation, de réagir au plus vite, mais surtout de construire l'ensemble des mécanismes qui vont permettre à l'entreprise de construire la confiance.

Comme on le dit souvent la confiance ne se décrète pas elle se construit, et il faut très peu pour la rompre. Un premier élément pour la confiance, s'appelle la certification ou la labélisation des services ou de l'entreprise. l'ISO 27001 est un des cadre de cette assurance sécurité.

chapitre à compléter, les éléments ne donnent qu'une vue trop réduite ou parcellaire du sujet

2

Eléments de Cryptologie

A une époque où chaque jour la presse se fait régulièrement écho de pertes ou de vols de données, où l'on continue à investir dans la protection des données personnelles, certains s'interrogent encore sur les moyens de protéger et partager de manière sûre son patrimoine informationnel. La cryptographie est une des disciplines de la cryptologie qui s'attache à protéger ces patrimoines en confidentialité, intégrité ou en authenticité. Il me paraissait intéressant de proposer en quelques mots, le vocabulaire et les concepts. Si la cryptographie est un outil pour deployer des mesures de sécurité, c'est aussi un ensemble de techniques utilisées par les attaquant. Au-delà des aspects mathématiques passionnants que nous ne traiterons pas ici, seuls quelques usages et arcanes techniques sont présentés.

2.1 Définitions

La cryptologie est par étymologie la science du secret. Elle regroupe la cryptographie, qui porte sur les moyens de coder et décoder les messages, et la cryptanalyse, qui permet de les déchiffrer (de manière non coopérative !). Ces techniques

remontent à la nuit des temps. Historiquement militaires et diplomatiques, elles sont devenues civiles avec l'avènement de technologies de l'information, dont la carte à puce [1] et l'internet.

Elles ont envahi à grande vitesse toutes les technologies numériques.« Signer, protéger, imputer, authentifier... » sont devenus des termes courants de cette vie numérique. On est toutefois surpris de l'usage, quelquefois un peu« dévoyé », de certaines expressions.« Crypter » s'oppose à« décrypter », mais si décrypter, c'est« décoder » sans connaître les secrets, crypter est humoristiquement enterrer mettre en« crypte »! Si les expressions« coder » et« décoder » sont régulièrement utilisées, celles préconisées sont « chiffrer » et « déchiffrer ». En France, au sein des armées, les acteurs du domaine se nomment d'ailleurs des spécialistes du chiffre [2]. Face à un spécialiste, du mathématicien cryptologue au commercial de services numériques de confiance, de nombreux termes se bousculent dans les discussions : algorithmes robustes de niveau militaire, clefs très longues, protocoles sûrs, certificats de confiance...

2.2 Concepts

Derrière ces arguments qui pourraient, au premier abord, paraître convaincants, il convient rapidement d'opposer une petite analyse terminologique et conceptuelle.

2.2.1 Algorithmes

Le nombre d'algorithmes mathématiques (fonctions mathématiques) en cryptographie est presque aussi grand que le nombre de mathématiciens qui travaillent dans le domaine. Il faut y ajouter le nombre d'implémentations informatiques de chaque algorithme, sans compter les différents langages utilisés pour la même implémentation. Quelques grandes révolutions ont eu lieu depuis le chiffre de César, mécanisme de chiffrement par décalage« alphabétique » utilisé dans notre enfance, et celui de la machine allemande Enigma de la dernière guerre, avec des mécanismes de substitution dits polyalphabétiques. Ces évolutions et révolutions

1. téléphonie mobile (SIM) et carte bancaire.
2. ARCSI : Association des réservistes du chiffre et de la sécurité de l'information - www.arcsi.fr

ont lieu chaque fois que ces fameux cryptanalystes trouvent ou entrevoient une solution pour casser ce chiffre... Une longue tradition dans cette course entre la cuirasse et le canon.

Chiffrement à clefs secrètes

Ces premiers algorithmes dits symétriques ou à clefs secrètes ont été et restent centraux, car ils se révèlent très rapides. Le principe est que pour déchiffrer, il faut simplement la clef qui a servi à chiffrer, d'où le terme« symétrique ». Une des grandes difficultés dans ces algorithmes est la combinatoire pour partager le secret. Si partager de manière sûre un secret entre deux ou trois correspondants est maîtrisable, le faire pour mille ne permet plus vraiment de parler d'une clef secrète ! L'histoire des célébrités technologiques retient des algorithmes comme DES, 3DES, IDEA, RC4 et le dernier réputé inviolé et issu d'un appel à projet du NIST [3] et paru dans les années 2000 : AES256.

Cryptographie à clefs publiques

Le chiffrement asymétrique résout ce problème de la combinatoire, mais reste bien plus lent. Rendu célèbre par Alice et Bob, deux personnages illustrant les cours de cryptologie asymétrique, ce mécanisme utilise une paire de clés liées dites asymétriques : une clé publique et une clé privée. La clé publique est rendue publique et distribuée librement. La clé privée n'est jamais distribuée et doit être gardée secrète. Pour cette une paire de clés, les données chiffrées à l'aide de la clé publique ne peuvent être déchiffrées qu'avec la clé privée correspondante (donc si vous avez la clef publique de votre correspondant, vous pouvez chiffrer une information pour lui). Inversement, les données chiffrées à l'aide de la clé privée ne peuvent être déchiffrées qu'avec la clé publique correspondante. Cette caractéristique est utilisée pour mettre en œuvre la signature numérique.

2.2.2 Fonction de hashage

Les fonctions de hachage cryptographique (de l'anglais« hash ») sont présentes dans tous nos systèmes numériques. Ce sont des fonctions rapides à sens unique qui permettent de transformer tout bloc d'information de taille quelconque et

3. National institute of standards and technology.

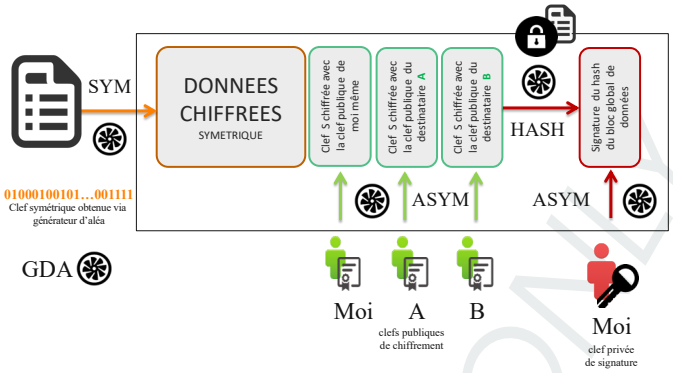

FIGURE 2.1 – Exemple d'une encapsulation asymétrique pour un chiffrement de fichier

une donnée de taille fixe souvent courte. Ce mécanisme, qui permet de prendre une« empreinte » des données, est à la base des mécanismes de signature, de contrôle d'intégrité et de stockage de mots de passe. Les algorithmes les plus connus sont md5, sha1 et maintenant sha256, sha512 nécessaires par les fragilités découvertes sur les premiers, car ces algorithmes sont aussi sujets aux attaques !

2.2.3 Clefs

Au cœur de la cryptographie, les clefs restent l'objet de toutes les attentions. Il est conseillé la lecture des quelques documents de référence de l'Anssi[4] sur les« mécanismes cryptographiques »[5] qui illustrent de manière pragmatique et concrète cette indispensable vigilance.

Taille de clefs

Un des débats dans l'usage de la cryptographie concerne la taille optimale des clefs. Ce sujet fait l'objet de nombreuses publications. Pour les algorithmes symétriques, 1 280 bits est la taille de référence (soient 2 puissance 128 possibilités). La notion de taille de clefs pour les algorithmes asymétriques est moins simple. Cela dépend des problèmes mathématiques sous-jacents. Pour le plus célèbre

4. Anssi : Agence nationale pour la sécurité des sytème d'information, services du Premier ministre.
5. Annexe B1 et B2 du RGS V2 (Anssi : référentiel général de sécurité) : Mécanismes cryptographiques et gestion des clefs.

RSA[6] (6), qui aura bientôt 40 ans, les experts considèrent qu'une taille de 2 048 est à l'état de l'art jusqu'en 2030. RSA est utilisé pour les transactions pour la carte bleue, les achats sur internet, les courriels sécurisés. Pour ceux basés sur le logarithme discret, la taille préconisée est de 200 bits, pour les courbes elliptiques de 256 bits. Il est donc important de spécifier les algorithmes pour comparer des tailles de clefs.

Aléas et générateur d'aléas

De nos jours, une bonne clef secrète est très rarement issue de notre cerveau (même un bon mot passe mémorisable est totalement perfectible sur le pur plan cryptographique)[7]. Pour générer des clefs d'un bon niveau cryptographique, c'est-à-dire non sujettes à des biais de prédiction possibles, il est nécessaire d'utiliser un générateur de nombres aléatoires (GDA ou RNG : « random number generator ») de qualité cryptographique. Il est fondamentalement complexe de générer de véritables nombres aléatoires. Le processus de génération d'aléas doit comporter des sources fondamentalement aléatoires (bruit électronique, thermique dans des composants) combinées à des sources multiples (hash d'une zone mémoire...), le tout passé à la moulinette d'algorithmes de pseudo-aléas suffisamment imprévisibles. Ce fondamental de la cryptologie est un domaine de recherche à part entière. C'est aussi une activité industrielle autour des HSM (hardware security module) pour la génération rapide, le stockage et la protection des clefs primordiales pour les transactions numériques bancaires en particulier.

Protocoles et formats

De bons algorithmes, de bonnes clefs ne suffisent pas. Il est indispensable de s'assurer de l'ensemble des mécanismes qui vont permettre de garantir que« les secrets échangés » restent bien secrets. On parle de protocole d'authentification, de signature, d'échange de clefs (Kerberos, Diffie Elmann, RSA...). C'est souvent au cœur de ces protocoles qui nécessitent une attention particulière en termes de robustesse et de preuve formelle que l'on trouve des vulnérabilités. Le format des données chiffrées (cf Fig. 2) est aussi une source de fragilité (cacher une partie

6. 1978, apparition de l'algorithme à clef publique de Rivest, Shamir et Adelman (RSA).
7. Un mot de passe de qualité« cryptographique » devrait être d'au moins 20 caractères dans un alphabet de 90 symboles.

de la clef en piégeant l'ordinateur, exploiter une vulnérabilité logicielle). Les solutions technologiques de chiffrement combinent pour des raisons de performance des mécanismes de chiffrement symétrique et asymétrique.

Certificats

Le terme« certificat électronique » est entré dans le langage courant du numérique :« Certificat machine, serveur »,« certificat utilisateur ». à la base des usages des systèmes à clefs publiques, ce certificat contient la (les) clef(s) publique(s), des informations d'identification, des dates de validité, et un mécanisme de signature garantissant l'origine. Informatiquement ce« paquet » de données nécessite des standards de formats structurés interopérables comme le codage X.509 ou le stockage PKCS12.

Certificats auto-signés !

Une clef publique« valide » dans un système cryptographique de confiance, doit être signée par une autorité de confiance pour être vérifiée par la suite par son« usager ». Disposer d'une PKI ou faire certifier sa chaîne de confiance est complexe et coûteux. Le monde informatique fait donc largement usage de l'auto-signature, c'est-à-dire de la génération des clefs, sans chaîne de confiance partagée. Lorsque les logiciels sont permissifs sur ces usages, l'ensemble du système est fragilisé.

IGC ou PKI

Utiliser des mécanismes à clefs publiques nécessite donc l'utilisation d'un ensemble interopérable de confiance (algorithmes, protocoles, formats) permettant de générer les clefs (couple privée/publique), de les attribuer, de les signer (les certifier), de les distribuer, et de les révoquer (les supprimer de l'environnement de confiance). L'ensemble de ces mécanismes s'appelle une IGC (infrastructure de gestion de clefs) ou PKI (public key infrastructure). Ces outils logiciels et l'organisation globale sont indispensables à un usage structuré de confiance. Sans cette maîtrise des clefs, un système à clef publique peut s'effondrer. En effet, si des clefs de certification, ou des clefs privées d'utilisateurs sont compromises à la source, la résistance mathématique des algorithmes ou des protocoles ne vous garantira plus grand-chose... C'est dans cet esprit que sont nés les tiers de confiance, qui

vous assurent que toutes les précautions sont prises pour protéger cette chaîne.

2.3 De la confiance aux usages en entreprise

Comme vous l'avez noté, un système cryptographique est un ensemble de briques (fig. 1) qu'il est nécessaire de contrôler pour définir un niveau de confiance de la chaîne. Si disposer d'outils à clefs publiques sans un IGC (PKI) se révèle fragile, disposer d'une IGC sans disposer d'une maîtrise des usages l'est autant... En France, le terme de moyen (9) cryptologique est défini par loi sur la confiance numérique, mais il est à remarquer que, dans l'entreprise, il se conjugue différemment en fonction des interlocuteurs :

- pour les équipes réseaux : la cryptologie est enfouie dans les méandres des protocoles des technologies des canaux sécurisés VPN, IPSEC, VPN, chiffreurs réseaux ;
- pour les équipes des services informatiques : le déploiement, la mise à jour des certificats sur des terminaux et des serveurs concentrent une bonne partie des problèmes opérationnels ;
- pour la bureautique et le poste de travail : les produits et les services pour chiffrer les données et préserver la confidentialité dans les messageries ou sur les supports (smartdevice, disques, USB, serveur de fichiers) sont complexes à choisir pour l'interopérabilité ;
- pour les métiers de l'entreprise comme les achats ou l'archivage probant, les enjeux d'authenticité, d'imputabilité et d'intégrité ainsi que la signature électronique nécessitent des travaux transverses à l'entreprise souvent coûteux.

Il est à noter, le point particulier du recouvrement des données chiffrées et du séquestre des clefs. Indispensable pour les malchanceux qui perdent leur clef privée ou par nécessité (départ de l'entreprise, réquisition sur des données...), la confiance dans celui qui possède cette capacité de recouvrement est un enjeu fondamental. Acquérir et déployer un système cryptographique dans l'entreprise doit se baser sur un minimum de confiance dans l'implémentation des briques. Il est important que ces produits aient été analysés, vérifiés par des tiers (entre le

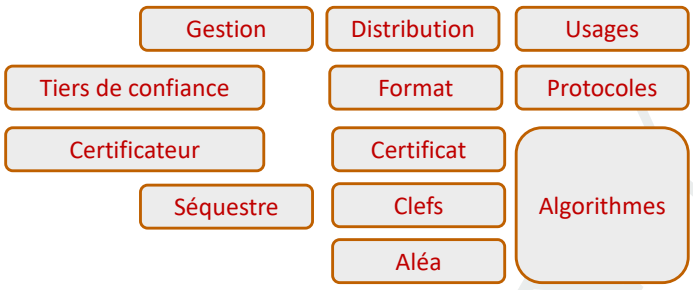

FIGURE 2.2 – Les briques à vérifier dans la chaine de confiance

constructeur ou éditeur et l'utilisateur ou acheteur). On parle ainsi de certifications de produits au titre de la norme de l'Iso 15408 (critères communs), qualification de produits et de services par l'Anssi. Perturbant un peu l'écosystème et les frontières de gouvernance des DSI, l'usage des services dans le cloud nécessite de nouvelles technologies de chiffrement pour maintenir la confidentialité totale, mais autoriser quand même des traitements. Le chiffre homomorphe permet justement à un système tiers d'opérer des calculs sur des données chiffrées sans les déchiffrer et ainsi récupérer les résultats exploitables. Des solutions matures arrivent sur le marché depuis peu.

2.3.1 De l'usure électronique au partage de confiance

Usure ou rupture cryptographique

Si le temps n'est pas l'ami de l'archivage, il ne l'est pas non plus du chiffrement. Non par l'usure du support, mais simplement par la complexité d'une longue conservation des clefs, de l'érosion de la résistance des mécanismes. En outre, depuis des années, le terme« quantique » est apparu dans la littérature du domaine. Si la distribution quantique offre une transmission sûre de clef, l'ordinateur quantique pourrait apporter cette rupture que redoute l'industrie numérique, car capable de rompre la solidité des problèmes mathématiques sur lesquels repose une grande partie des mécanismes cryptographiques actuels.

La cryptographie quantique est un espace de recherche de cryptographie qui utilise les propriétés quantiques de la matière pour sécuriser les communications et protéger les données. Elle repose sur des phénomènes quantiques tels que l'intri-

cation et la superposition, qui permettent de réaliser des calculs et des opérations de manière beaucoup plus rapide et plus efficace que les algorithmes classiques utilisés dans la cryptographie traditionnelle.

La cryptographie quantique est encore en développement et n'est pas encore largement utilisée dans les applications pratiques. Cependant, elle offre des avantages potentiels considérables en termes de sécurité et de vitesse de calcul. Par exemple, les algorithmes de cryptographie quantique pourraient être utilisés pour créer des clés de chiffrement plus sécurisées et pour effectuer des calculs complexes de manière beaucoup plus rapide que les algorithmes classiques.

Il est important de noter que la cryptographie quantique est également confrontée à des défis importants, notamment en ce qui concerne la stabilité des données quantiques et la difficulté à mettre en œuvre ces algorithmes de manière pratique. En outre, il existe des inquiétudes quant à la sécurité à long terme de la cryptographie quantique, car il est possible que de futurs progrès technologiques permettent de casser la confiance dans les chaines de confiance basée sur les algorithmes actuels de manière plus efficace.

En effet, si ces technologies sont pleinement mises en œuvre et deviennent largement utilisées, cela pourrait remettre en question la sécurité de nombreux systèmes de sécurité actuellement en place qui reposent sur des algorithmes de cryptographie classiques.

On peut citer les risques suivants

- Rupture de la sécurité de la cryptographie classique : Si les algorithmes de cryptographie quantique sont mis au point et deviennent largement utilisés, ils pourraient être utilisés pour cracker les codes de cryptographie classique, mettant ainsi en danger la sécurité de nombreux systèmes de sécurité actuels
- Compromission de la confidentialité des communications : Si les algorithmes de cryptographie quantique sont utilisés pour chiffrer les communications, ils pourraient être crackés par des parties malveillantes, compromettant ainsi la confidentialité de ces communications.

blockchain, Cyrpto-monnaies, NFT...

Nous avons rapidement parcouru l'usage courant de la cryptographie en entreprise, mais de nouvelles révolutions des usages de la cryptographie sont déjà à nos portes. Après quelques années d'hésitation, la montée des« crypto-monnaie » comme Bitcoin donne une large expression aux mécanismes de signature pour assurer intégrité, traçabilité, imputabilité et modifie le rapport à la confiance« centralisée ». Dans l'émergence rapide de cette« décentralisation de la confiance », quelques positions établies sont remises en cause. On notera en particulier une forme naissante d'ubérisation des chaînes de confiance, qui bouscule déjà le marché effervescent de la cybersécurité. Les chaines de confiance sont de plus en plus utilisé dans les cryto-monaies et NFT.

La cryptographie joue un rôle clé dans la sécurité et l'intégrité des blockchains en permettant de protéger les données et les transactions contre la modification ou la falsification. Ces actifs numériques à caractère authentique sont basés sur ces blockchains. Une blockchain est une base de données distribuée qui permet de stocker de manière sécurisée et transparente ces enregistrements de données. Elle est composée de blocs de données qui sont liés les uns aux autres de manière sécurisée grâce à l'utilisation de cryptographie.

Chaque bloc de la chaîne contient des informations sur les transactions qui ont été effectuées, ainsi que des données sur les blocs précédents. Lorsqu'un nouveau bloc est ajouté à la chaîne, il est vérifié et validé par plusieurs ordinateurs dans le réseau, ce qui rend la blockchain très difficile à altérer ou à falsifier.

Les blockchains sont principalement utilisées pour stocker et transférer des cryptomonnaies, mais elles peuvent également être utilisées pour d'autres applications, telles que la gestion de la chaîne d'approvisionnement, la gestion des actifs, la gestion de la santé, etc. Elles offrent un niveau élevé de transparence et de sécurité, ce qui les rend particulièrement utiles dans les situations où la confiance et l'intégrité des données sont importantes.

Les cryptomonnaies sont des formes de monnaies numériques qui utilisent la technologie de la blockchain pour sécuriser les transactions et contrôler la création de nouvelles unités de monnaie. Elles sont décentralisées, ce qui signifie qu'elles ne sont pas émises ni gérées par une banque centrale ou tout autre organisme gou-

vernemental.

La cryptomonnaie la plus connue est probablement le Bitcoin, qui a été créée en 2009. Depuis, de nombreuses autres cryptomonnaies ont vu le jour, chacune avec ses propres caractéristiques et utilisations. Certaines sont conçues pour être utilisées comme moyen de paiement, tandis que d'autres sont plus axées sur l'investissement.

Les cryptomonnaies sont souvent utilisées comme moyen de paiement en ligne et sont acceptées par certaines entreprises et commerçants en tant que moyen de paiement. Cependant, elles restent controversées en raison de leur manque de réglementation et de leur volatilité, avec des fluctuations de prix importantes pouvant survenir en très peu de temps. En outre, leur utilisation a été associée à des activités illégales en raison de la confidentialité qu'elles offrent aux utilisateurs.

Les NFT (Non-Fungible Tokens) sont en effet des tokens numériques qui représentent de manière unique des actifs numériques ou physiques. Ils sont stockés sur une chaîne de confiance basées sur des blockchains, comme la blockchain Ethereum, ce qui leur confère une certaine forme de rareté et de valeur.

Les NFT sont utilisés pour représenter des objets virtuels tels que des œuvres d'art numériques, des enregistrements de musique, des GIFs animés, des émoticônes, des personnages de jeux vidéo, etc. Ils permettent aux créateurs de ces actifs de monétiser leur travail de manière transparente et sécurisée, tout en offrant aux acheteurs la possibilité de devenir les propriétaires uniques de ces actifs.

Si les NFT sont de plus en plus populaires et suscitent beaucoup d'intérêt en raison de leur capacité à représenter de manière unique des actifs numériques, il est important de noter qu'il existe également des risques liés à l'achat et à la possession de ceux-ci. On note en particulier la confiance dans la sécurité globale dans ces blockchains ainsi que la stabilité et la liquidité du marché des NFT.

II

Références et Index

Références

Articles

(1) Sofia BARIM. « Développer la culture sécurité de l'information numérique de son organisation ». In : *I2D–Information, données & documents* 55.3 (2017), pages 49-50.

(2) Anton CHUVAKIN. « The complete guide to log and event management ». In : *White Paper* (2010).

(5) Quentin GAUMER. « Cybersécurité dans un contexte d'intelligence économique ». In : *I2D–Information, données & documents* 55.3 (2017), pages 32-33.

(6) Karen KENT et Murugiah SOUPPAYA. « Guide to computer security log management ». In : *NIST special publication* 92 (2006).

(9) Fred B SCHNEIDER. « Cybersecurity education in universities ». In : *IEEE Security & Privacy* 11.4 (2013), pages 3-4.

(10) Bruce SCHNEIER. « Attack trees ». In : *Dr. Dobb's journal* 24.12 (1999), pages 21-29.

(11) Lei SHEN. « The NIST cybersecurity framework : Overview and potential impacts ». In : *Scitech Lawyer* 10.4 (2014), page 16.

(12) Chee-Wooi TEN, Chen-Ching LIU et Govindarasu MANIMARAN. « Vulnerability assessment of cybersecurity for SCADA systems ». In : *IEEE Transactions on Power Systems* 23.4 (2008), pages 1836-1846.

Ouvrages

(3) Anton CHUVAKIN, Kevin SCHMIDT et Chris PHILLIPS. *Logging and log management : the authoritative guide to understanding the concepts surrounding logging and log management*. Newnes, 2012.

(13) Daniel VENTRE. *Cyberattaque et cyberdéfense*. Lavoisier, 2011.

index

Index

Aborder la sécurité des systèmes d'information sous l'angle d'une sécurité dynamique est un axe qui depuis quelques années apporte de nouvelle manière d'aborder la protection, la défense, et la résilience des systèmes d'information. La transformation digitale de l'entreprise modifie et rend plus flous les périmètres des systèmes d'informations. Cela nécessite une approche élargie du risque numérique et des nouvelles architectures de cybersécurité. Malgré la mise en place de mesures et de technologies de protection de plus en plus élaborées, l'impact d'une attaque ayant franchi ces barrières à considérablement augmenté. Cette compilation des notes de cours élaborée dans le cadre d'un cours d'introduction à la gouvernance de la cybersécurité aborde une démarche de cyberdéfense d'entreprise construite à partir de quelques éléments fondamentaux. Protéger l'ensemble de l'entreprise alors qu'il est complexe de définir ses frontières est illusoire. Identifier les actifs essentiels ou vitaux et mettre en place les moyens adaptés à leur protection et leur défense est une démarche tactique qui permet de graduellement réduire ses cyber-risques. Issu de ce cours sur le déploiement de politiques de cyberdéfense, cet ouvrage décrit quelques éléments essentiels de sécurité opérationnelle permettant de fixer, à partir d'une analyse des risques, des priorités opérationnelles tant sur l'organisation des processus que des architectures de protection, de défense et de résilience.

Eric DUPUIS (Enseignant SEC101, Cnam Bretagne) est actuellement Directeur d'Orange Campus Cyber, le centre de formation et d'entrainement Cybersécurité et Cyberdéfense du groupe Orange après plusieurs années comme directeur sécurité de la société Orange Cyberdefense. Ingénieur des corps techniques de l'armement du ministère des armées, il a exercé pendant plusieurs années à la Délégation Générale pour l'Armement / Maitrise de l'information (DGA/MI) dans les domaines du renseignement, de la lutte informatique et de la cyberdéfense.
Ingénieur du Conservatoire National des Art et Métiers, il y enseigne l'ingénierie et la sécurité du numérique. Auditeur de la 50ième session Armement et Economie de Défense de l'IHEDN (Institut des Hautes Etudes de la Défense National), il intervient au profit de la Gendarmerie, en tant qu'Officier de Réserve Cyberdéfense.

CYBERDEF 101