République Algérienne Démocratique et Populaire
Ministére de l'enseignement Supérieur et de la Recherche Scientifique
Université Constantine 2 – Abdelhamid Mehri
Faculté des Nouvelles Technologies de l'Information et la Communication
Département d'Informatique Fondamentale et ses Applications

Année : **2020**
Nº d'ordre :
Série :

MÉMOIRE

pour obtenir le diplôme

MASTER en Informatique

Option : Réseaux et Systèmes Distribués

. . . . . .

présentée et soutenue publiquement par

Karimou Seyni Ibrahim

le 25 mai 2020

Encadré par
Pr. Djamel Eddine SAIDOUNI, Directeur de mémoire
Dr. Bouneb Zine El Abidine, Co-encadreur

Jury
Dr. L. MEZAI , Présidente
Dr. Chaouche Ahmed-Chawki, Examinateur

MASTER

A ma mère
A mon père
A toute ma famille
A mes ami(e)s

Remerciements

Je tiens tout d'abord à remercier Allah, le Clément, le miséricordieux qui nous a permis de mener à bien ce modeste travail.

En premier lieu, je tiens à exprimer ma sincère gratitude à mon encadreur
Pr. Djamel Eddine SAIDOUNI, pour son intégrité, sa disponibilité, sa générosité de partager ses connaissances. Je voudrais lui témoigner ici toute ma gratitude pour m'avoir guidé durant ces périodes et laisse entrevoir ce que le mot recherche veut dire.

Je remercie chaleureusement **Dr. Bouneb Zine El Abidine** pour avoir accepté d'être mon co-encadreur, pour son soutien, ses nombreux conseils et l'intérêt qu'il a porté à mon travail.

Je souhaite exprimer toutes ma reconnaissance à mes parents qui m'ont soutenu tout au long de ces années et m'ont toujours encouragé de faire ce que je souhaitais et de donner le meilleur de moi-même.

Mes plus vifs remerciements s'adressent à tous les corps enseignants pour leur patience, leur dévouement pour nous avoir apporté le bagage nécessaire.

Je voudrais aussi exprimer mon amitié aux personnes avec qui j'ai eu le plaisir de partager ses années d'études et surtout ceux du premier et du second cycle.

Résumé

La vérification formelle constitue une étape indispensable pour garantir le bon fonctionnement des systèmes complexes et critiques. Le model checking est une technique efficace pour vérifier des propriétés sur des systèmes décrit avec un modèle formel. Ce pendant, cette méthode de vérification souffre d'un problème majeur engendré par l'explosion combinatoire de l'espace d'états à explorer dans un temps raisonnable.

Pour merdier a ce problème, la distribution de l'espace d'états est la solution la plus rependus en vue de tirer profit de la quantité de mémoire et de la puissance de calcul disponibles sur chaque machine. Par contre aboutir à une meilleur distribution pour accélérer la vérification s'avère être difficile a réalisé.

Notre travail réside dans la distribution de l'espace d'états, pour établir un compromis entre l'équilibrage de charge des différentes machines et la minimisation du taux de communications. Pour cela, nous proposons une nouvelle approche de distribution en avale de l'espace d'états basée la théorie de jeux et l'analyse des états. L'approche proposée vise à analyser l'espace d'états tout en extrayant les informations pertinentes sur les états. Ensuite, redistribuer les états suite à leurs pertinences soit migrés définitivement soit dupliqués sur d'autres machines, afin de minimiser le nombre de communications entre les machines. Cela est fait grâce à une stratégie comportementale de la théorie de jeux au quelle les machines cherchent à optimiser leur taux de communications tout en maintenant l'équilibrage de charge entre les machines à l'aide de seuils prédéfinis pour chaque machine. Ceci permet à une application d'optimiser ses comportements en cumulant ses expériences d'exécutions, ainsi grâce à l'utilisation des bases de données orientés graphes, les prochaines exécutions de l'application seront fait à partir des améliorations gagnées précédemment.

Mots clés : Réseau de Petri, Calcul parallèle, Structure de Kripke Distribué, Model checking distribué, Distribution des espaces d'états, Génération de l'espace d'états, Méthodes d'optimisation, Théorie de jeux.

Abstract

Formal verification is an essential step for ensuring the proper functioning of complex and critical systems. Model checking is an effective technique for checking properties on systems described with a formal model. However, this verification method suffers from a major problem caused by the combinatorial explosion of the states space to be explored in a reasonable time.

To solve this problem, the states space distribution is the most common solution to take advantage of the amount of memory and computing power available on each machine. On the other hand, it is difficult to obtain a better distribution to accelerate the calculation of the verification.

Our work lies in the distribution of states space, to establish a compromise between the load balancing of the different machines and the minimization of the communication rate. For this, we propose a new distribution approach in downstream of the states space based game theory and states analysis. The proposed approach aims to analyze the states space while extracting relevant state information. Then, redistribute the states following their relevance either migrated permanently or duplicated on other machines, in order to minimize the number of communications between the machines. This is done through a behavioral strategy of game theory in which machines seek to optimize their communications rate while maintaining load balancing between machines using predefined thresholds for each machine. This allows an application to optimize its behavior by combining its execution experiences, and thanks to the use of graph-oriented databases, the next executions of the application will be made from the improvements previously gained.

Keywords : Petri Net, Parallel Computing, Distributed Kripke Structure, Distributed Model Checking, State Space Distribution, State Space Generation, Optimization Methods, Game Theory.

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Introduction

Les progrès fulgurants des Technologies de l'Information et de la Communication(*TIC*) et le bésoin de faire collaborer des objets ont conduit à un concept moderne qui est « Internet of Things» (*IoT*). L'IoT nous offre une nouvelle opportunité de croissance nous permettant délimiter la perte de temps, de ressource, améliorant ainsi nos vie quotidiennes. De nos jours, il existe de nombreuses plateformes et applications pour l'IoT conduisant à fournir de nouveaux services et automatiser de nombreux processus dans l'industrie(smart industry), la santé(smart health), le ménage, les transports(smart transport) et de nombreux autres secteurs.

Il existe plusieurs définitions sur le concept de l'IoT, mais nous adoptons celle proposée par Weill et Souissi qui ont défini l'IoT comme « une extension de l'Internet actuel envers tout objet pouvant communiquer de manière directe ou indirecte avec des équipements électroniques eux-mêmes connectés, à l'Internet. Cette nouvelle dimension de l'Internet s'accompagne avec de forts enjeux technologiques, économiques et sociaux tout en assurant la protection des données des utilisateurs » [Zhang Hang, 2013]. Quasiment n'importe quel appareil doté d'un bouton marche/arrêt peut se connecter à l'Internet aujourd'hui, intégrant ainsi la catégorie des objets de l'IoT [kaspersky]

En ce qui concerne l'IoT, Les objets connectés peuvent être des objets physiques ou virtuelles (smartphones, ordinateurs, data centers, réseaux Wi-Fi, réseaux cellulaires, puces RFID , capteurs, équipement ménager, montres, serrures, véhicules, drones, etc) pouvant être identifiés et intégrés dans la communication des réseaux. D'après la plateforme statisca [statista, 2020] aujourd'hui le nombre d'objets connectés est estimé à $30.73 milliards$ d'objets connectés dans le monde et ce nombre atteindrait les 75.44 $milliards$ d'objets connectés en 2025.

Cependant assurer la confidentialité, la disponibilité et l'intégrité des objets connectés ainsi que les données qui y transitent sont les principales préoccupations concernant l'adoption de ce nouveau concept l'IoT. Une fois que les appareils sont connectés à Internet, ils deviennent vulnérables à d'éventuelles d'attaques informatiques. l'IoT étant la prochaine génération d'Internet [Dave, 2011] avec de plus en plus d'objets connectés allant des villes connectés aux vaches connectées. Dans ce réseau les objets connectés s'échangent des informations pour répondre à un but bien défini. Cette collaboration des objets ouvre des portes d'attaques aux hackers qui effectuent des attaques de plus en plus sophistiquées.

Selon 451 Research [Buckley] beaucoup d'entreprises sont toujours retissant dans l'adoption de l'IoT à cause sa gestion de la sécurité de ce nouveau qui est encore en état embryonnaire, mais 55% des entreprises qui ont adoptées l'IoT classent la gestion de la sécurité IoT comme leur priorité absolue lors des déploiements de projets IoT au sein de leurs organisations. Les systèmes vulnérables des objets connectés peuvent être compromis de n'importe où et utilisés pour cibler n'importe qui raison pour laquelle la sécurité IoT est une préoccupation mondiale.

Les objets connectés font faces à plus types de menaces. ces types de menaces sont classées en quatre(4) types [infosec] :

— **Déni de Service :** Cette menace vise la disponibilité d'un service ou d'une ressource en la saturant de requête indésirable empêchant ainsi ses utilisateurs légitimes de

l'utiliser. cette indisponibilité du service ou d'une ressource est mise en œuvre avec par l'attaque de types DDoS. C'est probablement l'une des ménaces les plus courantes et les plus dangereuses .

— **les logiciels malveillants** Un auteur de malware conçoit spécifiquement ses codes pour compromettre les architectures utilisées par les appareils IoT. Un code malveillant pourrait être utilisé pour infecter les ordinateurs utilisés pour contrôler un réseau d'appareils intelligents ou pour compromettre le logiciel qui y est exécuté. Dans ce deuxième scénario, les attaquants peuvent exploiter la présence d'une faille dans le micrologiciel exécuté sur les appareils et exécuter leur code arbitraire, transformant les composants IoT en utilisation non planifiée [infosec]

— **Violation de données (Data Breaches) :** C'est une menace visant l'intégrité et la confidentialité des données. les attaquants peuvent utiliser des attaques de type homme du milieu pour intercepter les communications des objets connectés.

— **Affaiblissement des périmètres :** Les appareils de l'Internet des objets ne sont généralement pas conçus pour la sécurité. Bien qu'il s'agisse d'appareils connectés à Internet, la majorité des appareils ne disposent pas de mécanismes de sécurité réseau. Prenons, par exemple, un compteur intelligent. Si l'attaquant est en mesure de le compromettre, il pourrait avoir accès à notre réseau domestique, nous espionner ou causer des dommages physiques à notre environnement domestique. Le problème est tout aussi grave si nous considérons l'utilisation d'appareils IoT dans n'importe quelle industrie.[infosec]

Contribution

Nous nous focaliseront dans ce mémoire sur la menace « déni de service », notamment l'attaque par Déni de Service Distribué (*DDoS*). Une attaque par déni de service distribué est une attaque qui empêche l'accès à une ressource ou à un service internet. Elle est obtenue en saturant avec des centaines de milliers voire des millions de connexions(requêtes) un serveur ou un objet connecté jusqu'à le bloquer.

À titre d'exemple :

— En 2007 l'Estonie [Jégo, 2007] a été victime de la première plus grande attaque DDoS de l'histoire. l'attaque visait le système informatique du pays notamment ses sites gouvernementaux, ses banques et ses médias créant la panique et déclenchant de vaste d'émeute au sein de la population et force de l'ordre.

— En octobre 2016 [Strawbridge] Dyn un important fournisseur de service de noms de domaine a été victime d'une vague d'attaque par déni de service distribuée. l'attaque était orchestrée à l'aide d'un logiciel malveillant appelé Mirai, les pirates se sont servis de ce programme pour créer un énorme botnet de 100000 objets connectés pour lanceur leur attaque. L'attaque a été extrêmement perturbatrice et a fait tomber les sites Web de plus de 80 de ses clients, notamment Amazon, Netflix, Airbnb, Spotify, Twitter, PayPal et Reddit. Les dommages causés par cette attaque auraient coûté $110 millions$ de dollars ainsi que la dégradation de la réputation du fournisseur.

— En 2018 github, une plateforme de développement à son tour était visée d'attaque DDoS qui a été. l'attaque a été maitrisée 10 min après [Strawbridge] grâce à la présence système de protection d'attaque DDoS dans la plateforme.

Nous proposons dans ce mémoire la mise en place d'un système de détection d'intrusion dans le réseau IoT contre les attaques de types DDoS. Afin d'assurer la disponibilité d'un service ou d'un objet connecté dans le réseau IoT. Notre choix du DDoS s'explique du fait que le DDoS utilise les objets connectées non sécurisés pour sa mise œuvre et du fait qu'elle est actuellement considérée comme l'attaque la plus dangereuse visant l'IoT [Adat u. a., 2017] Perakovic u. a. [2015].

Plan du document

Conformément à ce qui vient d'être exposé, le manuscrit se décompose en deux parties :

La première partie : présente l'état de l'art sur les différents domaines entrant en jeu dans le cadre de ce mémoire à savoir la sécurité informatique et la cybersécurité, l'attaque par déni de service distribué (**DDoS**), l'Internet des objets(**l'IoT**).

La seconde partie :

Première partie

Contexte de travail

Chapitre 1

SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

Sommaire

1.1 Introduction

Dans un monde de plus en plus connecté, où l'économie mondiale dépend de plus en plus de l'utilisation des services d'Internet, des services numériques, ainsi que les technologies émergentes sont davantage ancrées dans les économies du monde, il est absolument essentiel d'assurer une cybersécurité efficace. Tant que l'utilisation des TIC progressent, les risques augmentent aussi. Il s'agit donc de répondre à des défis et des cybermenaces qui ne cessent d'évoluer, ce qui exige que tous les acteurs soient au courant des facteurs de risque, qu'ils disposent des capacités nécessaires et qu'ils prennent les mesures appropriées en matière de prévention et de résolution. Pour garantir un cyberespace sûr, résilient et sécurisé les pays doivent explorer la réalité complexe et multisectorielle de la cybersécurité ce qui soulève des questions stratégiques, techniques, juridiques, de politique et de sécurité, et qui suppose l'établissement d'une collaboration multisectorielle et internationale.

Aujourd'hui notre mode de vie ultra connecté ne peut se passer des objets connectes et comme une connexion à un réseau rend possible une intrusion. Le fait d'interconnecter des objets augmentent d'autant plus la surface d'attaque aux cyber attaquants nous rendant ainsi beaucoup plus vulnérables.Cette multiplicité d'objets, de connexions, et de règlementation fait qu'aujourd'hui qu'il est difficile d'appliquer un seul modèle de sécurité. Le cyber espace est donc un monde à hauts risques d'attaques. Le mot anglais « Security » signifie une résistance à une malveillance, se traduit en français par « sûreté », alors que le mot « safety » signifie une résistance à une panne.

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. C'est une branche de la technologie de l'information qui étudie et met en oeuvre les menaces et les vulnérabilités des systèmes informatiques.
La cybersécurité est la partie de la sécurité informatique qui assure la protection du cyberespace contre les cybers menaces. Le terme cybersécurité n'est pas synonyme de sécurité informatique (1). La cybersécurité s'applique aux systèmes interconnectés, du fait que l'information numérique à protéger voyage à travers eux et y réside en eux. (2).

1.2 Les objectifs de sécurité informatique

La notion de sécurité d'un système informatique s'exprime généralement en termes de **disponibilité (D), d'intégrité (I) et de confidentialité (C) (3)**. Ces critères (dits critères DIC) sont les objectifs de sécurité de base dont leurs mises en oeuvre permettent d'atteindre un certain niveau de sécurité. En plus de ces fonctions s'ajoutent d'autres services de sécurité complémentaires pour confirmer **la véracité ou l'authenticité** d'une action ou d'une ressource (notion d'authentification) ou encore pour prouver l'existence d'une action à des fins de **non-répudiation ou d'imputabilité**, ou de **traçabilité**.

Un service de sécurité est un service qui augmente la sécurité des traitements et des échanges de données d'un système. Les critères de disponibilité, de confidentialité et d'intégrité sont à satisfaire par des mesures appropriées afin de pouvoir atteindre un certain niveau de confiance dans les contenus et le fonctionnement des infrastructures in-

formatiques et télécoms.

1.2.1 La confidentialité :

La confidentialité consiste à rendre l'information inintelligibles aux acteurs illégitimes d'une transaction ou d'une communication. Elle garantit l'anonymat des données en limitant leurs accès par le chiffrement et l'authentification.
La confidentialité assure que seules les personnes autorisées peuvent accéder à l'information. Les politiques d'entreprise devront limiter l'accès à l'information au personnel autorisé et garantir que seules ces personnes autorisées consultent ces données. Les données peuvent être compartimentées selon le niveau de sécurité ou de sensibilité de l'information.
Par ailleurs, les employés doivent suivre une formation pour comprendre les bonnes pratiques en matière de protection des informations sensibles pour se protéger et pour protéger l'entreprise contre les attaques. Il existe deux méthodes complémentaires permettant d'assurer la confidentialité :

- Limiter et contrôler l'accès aux données afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- Rendre inintelligibles les données en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser. Cette tache est réalisée en utilisant le chiffrement (cryptographie).

1.2.2 L'intégrité :

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication. L'intégrité représente l'exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie. Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions, services) assure qu'elles demeurent intactes, qu'elles n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires tant de manière intentionnelle, qu'accidentelle.

Préserver l'intégrité des ressources et s'assurer que des ressources sont intègres sont l'objet de mesures de sécurité. Ainsi, se prémunir contre l'altération des données et avoir la certitude qu'elles n'ont pas été modifiées collabore à la qualité des prises de décision basées sur celles-ci. Si en télécommunication, l'intégrité des données relève essentiellement de problématiques (4)liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciels d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données). L'intégrité des données est mise en oeuvre par des mécanismes cryptographiques et les signatures numériques pour s'assurer que les données n'ont pas été victimes d'écoute ou d'altération lors de leur transfert par des cyberattaques

1.2.3 La Disponibilité :

La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel. Elle garantit la continuité à l'accès à un service ou à des ressources. Le volume potentiel de travail susceptible d'être pris en charge durant

la période de disponibilité d'un service détermine la capacité d'une ressource à être utilisée. Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit (notion d'accessibilité).

La disponibilité des services, systèmes et données est obtenue par une maintenance des équipements, la réparation des matériels, la mise à jour des systèmes d'exploitation et des logiciels, la création de sauvegardes ainsi que l'utilisation d'équipements ou de service de sécurité. Les attaques de types **DoS** et **DDOS** peuvent causer l'indisponibilité d'un service ou d'une ressource. Celles-ci, sont possibles si les procédures de sauvegarde et de restitution ainsi que les supports de mémorisation associés ne sont pas gérées correctement ou s'il y a malveillance. Une politique de sauvegarde et des systèmes de détection d'attaques de types **DDOS** doivent être mis en oeuvre pour éviter le risque d'indisponibilité d'un service ou d'une ressource.

1.2.4 La traçabilité :

L'enregistrement des activités permettent la traçabilité des événements et leur analyse. Garder la mémoire des actions survenues permet notamment de reconstituer et de comprendre ce qui s'est passé lors d'incidents afin d'améliorer la sécurité, d'éviter que des erreurs ne se répètent ou d'identifier des fautifs. Cela autorise par exemple d'analyser le comportement du système et des utilisateurs à des fins d'optimisation, de gestion des incidents et des performances ou encore d'audit.
L'enregistrement des actions et événements permet également d'enrichir les bases de données qui permettent de développer des applications de surveillance, de détection et de réaction aux incidents, en particulier à l'aide des techniques issues de l'intelligence artificielle.

1.2.5 L'authentification et l'identification :

L'identification consiste à attribuer une identité unique à un utilisateur. Elle permet de répondre à la question : *Qui êtes-vous ?*ssi.ac strasbourg.fr.. Pour se faire l'utilisateur utilise un identifiant unique qu'on nomme Compte d'accès (Nom d'utilisateur ou Login en anglais). L'authentification consiste à assurer la véracité de l'identité d'un utilisateur. Elle permet de répondre à la question : *êtes-vous réellement cette personne ?* ssi.ac strasbourg.fr. Pour se faire l'utilisateur utilise un authentifiant ou code secret (mot de passe ou password en anglais) dont lui seul à la connaissance.
L'identification et l'authentification des ressources et des utilisateurs permettent d'associer la réalisation d'une action à une entité qui pourra en être tenue responsable et éventuellement en rendre compte. Un contrôle d'accès permet l'accès à des ressources uniquement aux personnes autorisées à travers un mot de passe crypté.

1.2.6 La non-répudiation et l'imputabilité :

La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier une transaction, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il prête être en d'autres termes assurer la preuve d'origine ou de destination de message.

L'imputabilité est la possibilité d'attribuer la responsabilité d'une infraction à un individu. Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes relatives à un événement. La non-répudiation et l'imputabilité sont assurer en utilisant les algorithmes de chiffrement asymétriques.

1.3 Application de la sécurité informatique :

La sécurité contient une variété de contextes et dépends du domaine d'application. On distingue 6 catégories de sécurité en fonction du domaine d'application (Figure 3) :

- **Sécurité matérielle physique et environnementale**;
- **Sécurité logique et applicative**;
- **Sécurité de l'information**;
- **Sécurité de l'exploitation**;
- **Sécurité des réseaux**;
- **Cybersécurité**.

1.3.1 La cybersécurité :

Le mot *Cybernétique* vient du grec « kuberneïn » qui signifie *diriger ou gouverner*, terme repris en 1948 par le mathématicien **Norbert Wiener** ancien professeur du Massachusetts Institute de Technologie (MIT) qui l'a publié pour la première fois dans son ouvrage intitulé Cybernetics, or Control and Communication in the Animal and the MachineWiener [1948].
Plusieurs décennies plus tard l'auteur de science-fiction William Gibson utilise le terme de cyberespace dans son roman le Neuromanien. Il s'agit d'une trilogie qui a pour personnage central un voleur de données. Celui-ci est à mesure d'établir des connexions entre son esprit et un réseau mondial liant des ordinateurs entre eux William [1984].
Au fuir du temps le préfixe *cyber* va participer ainsi à la construction de nouveaux mots lui donnant une nouvelle définition. Cyber est un préfixe servant de créer de mots relatifs à l'utilisation d'internet et à cette société de l'information qui a vu le jour à la fin du XXème. Aujourd'hui il y a plus de 40 mots débutants par Cyber dont : Cybersécurité, cybernétique, cyberespace, cybercafé, cybercrime, cyberattaque, cyberdéfense, cyberguerre, cyberterroriste, cybermonde etc.
Aujourd'hui avec l'utilisation extensif d'Internet des objets générant de nouveaux types de menaces dont seule la cybersécurité peut y faire face.

La cybersécurité est la partie de la sécurité informatique qui protège le cyberespace contre les cybers attaques. Elle concerne la sécurité des systèmes accessibles via le cyberespace(internet)et englobe la sécurité de l'information, la sécurité des réseaux et des environnements connectés. Le cyberespace est un espace virtuel relatif à notre espace naturel en d'autres termes un ensemble d'infrastructures numériques, de données et services misent en réseaux mais contrairement à la terre, à la mer, à l'air et à l'espace-extra atmosphérique, le cyberespace est une pure création de l'être humain qui ne relève pas de la nature Solange [2019]. Le terme cybersécurité est large et englobe chaque élément, de la sécurité de l'ordinateur à la reprise de l'activité après sinistre et la formation des utilisateurs kaspersky.

1.3.2 La sécurité des réseau :

La sécurité d'un réseau consiste à protéger un réseau informatique contre les intrus, qu'il s'agisse d'attaques ciblés ou de logiciels malveillants en d'autres termes protéger les équipements, les applications et les données du réseau contre les cybers attaques. Elle utilise plusieurs services et protocoles de défense allant de la couche physique à la couche application. Pour se faire plusieurs approches sont utilisés dans le modèle **TCP/IP** comme décrit ci-dessous :

- Couche transport (protocoles TLS/SSL, SSH),
- Couche internet (protocole IP Sec) ;

1.3.2.1 Protocoles TLS/SSL :

TLS de l'acronyme **T**ransport **T** **L**ayer **S**ecurity et **SSL** de l'acronyme **S**ecure **S**ocket **L**ayer, sont des protocoles de chiffrement qui garantissent la sécurité des échanges de données via un réseau informatique. Ils sont largement utilisés pour la sécurisation des communications sur internet.
Ils utilisent les techniques de chiffrements asymétriques et des algorithmes de cryptage

comme RSA, ECC, pour assurer la confidentialité, l'intégrité des données ainsi que l'authentification et l'identification des utilisateurs.

1.3.2.2 Le protocole IPSec :

IP Sec pour Internet Protocol Security est une suite de protocoles normalisés par L'Internet Engineering Task Force (**IETF**) qui fournit des services de sécurisations des données dans un réseau IP au niveau de la couche réseau. Fondé dans le but d'assurer la sécurité du protocole IPv6 et a été réadapter par la suite au protocole IPv4. Il assure les critères de confidentialité, d'authentification et d'intégrité des données échangées à travers un réseau IP ainsi qu'à la création de réseau privé virtuel (**VPN**).
L'**IPSec** peut fonctionner en deux : mode transport et mode tunnel. Le mode transport est utilisé pour les communications de bout en bout (Host to Host). Le mode tunnel est utilisé pour les configurations passerelle à passerelle ou passerelle à hôte (Gate-to-Gate ou host-to-Gate)MARWA [2016].

En plus de ces protocoles il existe plusieurs moyens classiques pour protéger un réseau informatique dont : les firewalls, la segmentation du réseau, les anti-virus et anti-malwares, les contrôles d'accès réseaux, les zones démilitarisés (DMZ) dont nous détaillerons dans la section mécanismes de sécurité.

1.3.3 La sécurité logique et applicative :

La sécurité des applications se concentre sur la protection des logiciels et des appareils contre les menaces. Une application compromise pourrait fournir un accès aux données qu'elle est destinée à protéger. Une sécurité réussie commence au stade de la conception, bien avant le déploiement d'un programme ou d'un périphérique.
La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle s'appuie généralement sur :

- La qualité des développements et l'implémentation des logiciels et des tests de sécurité ;
- Une mise en oeuvre adéquate de la cryptographie pour assurer intégrité et confidentialité ;
- Des procédures de contrôle d'accès logique, d'authentification ;
- Des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents ;
- La sécurité applicative comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.

1.3.4 La sécurité des informations :

La sécurité de l'information est un ensemble de stratégies de gestion et politiques de sécurités visant à protéger, détecter, recenser et contrer les menaces ciblant les données. Une donnée est la représentation d'une information. Elle vise à protéger des données et s'applique à tous les aspects de la sûreté, l'intégrité, la disponibilité et la confidentialité, la garantie, et la protection d'une donnée ou d'une information quelle que soit sa forme,

tant en stockage qu'en transit kaspersky..

Le système d'information étant le maillon de l'entreprise, l'information qui y transite doit être impérativement protéger contre le vol, la destruction et la falsification d'information pouvant causer d'énorme pertes à l'entreprise. Une classification des données permet de qualifier leur degré de sensibilité (normale, confidentielle, etc.) et de les protéger en fonction de ce dernier

1.3.5 La sécurité d'exploitation :

La sécurité de l'exploitation est un ensemble de stratégies de gestion et de politiques de sécurités visant à assurer le bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jourSolange [2019]. Elle s'appuie sur les différents mécanismes et services de sécurités suivants :

- Une gestion des systèmes d'exploitation, des configurations et des mises à jour ;
- Gestion des incidents et suivi jusqu'à leur résolution ;
- Une politique de sauvegarde, de secours, de continuité et de tests ;
- Gestion des contrats de maintenance ;
- Une analyse des fichiers de journalisation et de comptabilité

1.4 Les types de menaces et d'attaques :

Une menace est une cause potentielle d'incident, qui peut provoquer un dommage sur un système et ayant un impact sur ses fonctionnalités, son intégrité ou sa disponibilité. Une cybermenace est une menace qui s'exprime via le cyberespace, qui peut toucher tout système connecté à Internet dont sa concrétisation par une cyberattaque, peut affecter le bon fonctionnement des ordinateurs, des réseaux de télécommunication et de tous les services et activités humaines qui en dépendent. Les cybermenaces sont le plus souvent associées à l'usage malveillant des technologies Internet et à la cybercriminalité. De nombreuses cyberattaques existent, elles recouvrent des réalités diverses en fonction des cibles touchées, de leurs impacts, finalités, origines et auteurs.

1.4.1 La cybercriminalité :

Selon Colin ROSE « La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires » ROSE [2000]. Le cout global de la cybercriminalité est estimé à 6000 milliards de dollars et triplera le nombre d'emplois non pourvu en cybersécurité d'ici 2021 pandasecurity.
La cybercriminalité est toute infraction impliquant l'utilisation des technologies informatiques. Elle comprend des acteurs uniques ou des groupes ciblant des systèmes à des fins de gain financier ou de perturbation. Malgré que les entreprises et les forces de l'ordre tentent de s'attaquer au problème croissant, le nombre de cybercriminels continue de croître, profitant de l'anonymat d'Internet.
La cybercriminalité se divise en trois grandes catégories : la cybercriminalité individuelle, la cybercriminalité contre la propriété et la cybercriminalité gouvernementale pandasecurity

La cybercriminalité individuelle est une catégorie de cybercriminalité dont le criminel utilise des informations et programmes malveillants pour arriver dans le but de nuire à un individu.

La cybercriminalité contre la propriété est la catégorie de cybercriminalité dont le criminel s'usurpe (vol d'identité) de l'identité d'une personne. Une fois le criminel possède les informations personnelles volées il procède à des achats, des élévations de privilèges afin d'accéder à des informations confidentielles ou au chantage.

La cybercriminalité gouvernementale est l'infraction la plus grave qui consiste à un crime contre le gouvernement, par exemple le piratage de site web gouvernementaux ou de la diffusion de propagande. Ces genres de cyberattaques sont menés par des terroristes ou dans le cadre d'une cyberguerre entre nations.

1.4.2 DDoS (Distributed Denied of Service) :

Le **DDoS** est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. La ressource peut être une seule machine (comme un serveur), un groupe de machines(comme un pool de serveurs dédiés), voire un réseau Muhammad Aamir1 [2019]. Le **DDoS** est actuellement l'une des attaques la plus dangereuse pour les états, les entreprises causant beaucoup de perte d'argent et même en vie humaine si elle est bien structurée et visant des infrastructures critiques. Voilà pourquoi nous avons choix de nous focaliser sur ce type d'attaque. Le chapitre suivant est consacré entièrement à l'attaque **DDoS**.

1.4.3 L'ingénierie sociale :

L'ingénierie sociale est un ensemble des techniques de manipulation psychologique ou d'exploitation comportementale d'un individu, ou d'un groupe d'individus, par des personnes malfaisantes dont le but est l'incitation à amoindrir, contourner ou supprimer les mesures de sécurité d'un système par ce ou ces individus kaspersky [2020].

L'ingénierie sociale se sert en général des comportements ou de la personnalité particulière de leurs cibles tels que la naïveté, les émotions personnelles, les centres d'intérêt, L'adresses e-mail, la serviabilité, la confiance, le respect, la fierté, la reconnaissance dans le but de s'emparer de leurs accès informatiques. Elle procède comme suite :

— Collecte d'information,

— Etablissement de relations,

— Exploitations des vulnérabilités identifiées,

— Et ensuite l'exécution.

Les types d'attaques d'ingénierie sociale les plus utilisées sont : l'hameçonnage, le vishing, etc.

1.4.3.1 L'Hameçonnage :

L'hameçonnage ou phishing en anglais est l'une les plus courantes des attaques d'ingénierie sociale. C'est un courriel frauduleux ou un faux site conçu en usurpant l'identité d'un individu ou d'une organisation pour inciter leurs cibles à révéler des informations

privées (nom d'utilisateur, mots de passe, information de cartes de crédit, etc.) ou télécharger des logiciels malveillants.

Les courriels d'hameçonnage reposent sur des tactiques de peur, comme des courriels urgents de votre banque ou d'une autre institution financière, ou de votre patron, comme des offres de produits bon marché ou difficiles à trouver ou votre sens du devoir envers votre patron. Ça pourrait être aussi un faux site web contrôler par l'attaquant, usurpant d'un site officiel incitants les utilisateurs à fournir leurs informations personnelles.

1.4.3.2 Le vishing :

Le vishing ou attaque par téléphone est la version téléphonique de l'hameçonnage et la plus facile à mettre en oeuvre, c'est une technique frauduleuse utiliser par les pirates pour récupérer des informations (généralement bancaires) auprès d'utilisateurs de téléphone portable.

Les hackers qui utilisent cette technique préparent soigneusement leur personnage et leur discours, au préalable et ensuite appeler leur cible dans le but d'obtenir des renseignements le plus rapidement possible. Certains pour parfaire leur crédibilité, utilisent un magnétophone ou une cassette préalablement enregistrée de bruits de bureau, ou encore utiliser un matériel qui change le timbre de la voix pour imiter celle d'une secrétaire ou d'un patron.

1.4.4 Attaque par brute force et par dictionnaire :

L'objectif de ces attaques est généralement le même ; deviner le bon mot de passe ou de décrypter un texte en utilisant des tentatives, des techniques et des logiciels de décryptage. Elle se base sur la philosophie *n'importe quel mot de passe est crackable ce n'est qu'une question de temps.*

L'attaque par force brute de l'anglais **brute force cracking** consiste à tester de façon exhaustive toutes les combinaisons possibles de caractères (alphanumérique, symbole) de manière à trouver un mot de passe valide. Elle se base sur le fait que n'importe quel mot de passe est crackable ce n'est qu'une question de temps.
L'attaque par dictionnaire consiste à cracker un mot de passe en se basant sur document répertoriant des mots courants, des prénoms, des noms d'animaux ou des objets etc. Les outils d'attaque par force brute peuvent demander des heures, voire même des jours ou des années, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « attaque par dictionnaire » souvent vue comme un complément de l'attaque par brute fore. En effet, la plupart du temps les utilisateurs choisissent des mots de passe ayant une signification réelle. Avec ce type d'attaques, un tel mot de passe peut-être craquer en quelques minutes

1.4.5 Attaque par Homme du milieu :

Attaque par homme du milieu (**HDM**) ou man-in-the-middle en anglais (**MITM**) est une attaque par laquelle un attaquant accède aux communications entre deux noeuds légitimes, sans qu'aucune de ces deux noeuds ne s'en rende compte. L'attaquant peut lire le contenu de la communication, parfois les modifier. Pour se faire l'attaquant passe généralement par une connexion internet et doit donc être capable de recevoir les messages

(les décrypter s'ils sont chiffrés) des deux parties et d'envoyer des réponses à une partie en se faisant passer pour l'autre futura sciences [2020].

1.4.6 Logiciels Malveillants (Malware) :

Un logiciel malveillant est un type de logiciel conçu pour obtenir un accès non autorisé ou pour endommager un ordinateur. Logiciel malveillant qui comporte un ensemble de programmes conçus par un pirate pour être implantés dans un ordinateur à l'insu de l'utilisateur. I1 regroupe les virus, vers, spywares, keyloggers, chevaux de Troie, backdoors etc.

1.4.6.1 Les virus :

Un virus informatique est un programme ou un code malveillant qui est chargé dans votre ordinateur à votre insu sans votre autorisation. Certains virus sont seulement désagréables, mais la plupart sont destructeurs et sont conçus pour infecter les systèmes vulnérables et en prendre le contrôle.

Les virus sont généralement attachés à un fichier exécutable ou un document Word. Ils se propagent souvent via le partage de fichiers en P2P, de sites Internet infectés et le téléchargement de pièces jointes. A l'interaction avec ces fichiers infectés par exemple le clic sur un fichier, l'ouverture d'un fichier ou à l'exécution d'un programme, le virus s'exécute automatiquement et s'installe dans l'ordinateur de la victime. Une fois qu'un virus pénétré dans votre système, il restera en dormance jusqu'à l'activation du programme ou du fichier hôte infecté, qui à son tour activera le virus et lui permettra de s'exécuter et de se reproduire sur votre système kaspersky [2020].

1.4.6.2 Chevaux de Troie :

Le cheval de Troie est un logiciel qui ne se reproduit pas et permet d'ouvrir une « porte » sur l'ordinateur de la victime pour en prendre ultérieurement le contrôle ou activer à distance des programmes nocifs appelés « malwares ».

Encore appelé « Trojan Horse » en anglais, ce type de logiciel n'est rien d'autre que le véhicule, celui qui fait entrer le programme malveillant à l'intérieur de la machine. Il n'est pas nuisible en lui-même car il n'exécute aucune action, si ce n'est de permettre l'installation du vrai programme malveillant. Très présent dans les pièces jointes de messagerie, ces programmes sont souvent destinés au vol de données personnelles, et notamment financières.

1.4.6.3 Les keyloggers :

Il s'agit d'enregistreurs de frappes de touche du clavier d'un ordinateur dont les informations sont ensuite adressées au pirate agissant à distance. Il lui est ainsi possible de connaître les informations sensibles de sa victime comme des références bancaires ou toutes autres données qui lui permettraient de commettre ultérieurement une escroquerie.

Certains keyloggers sont capables d'enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute

l'activité de l'ordinateur infecté. Ils peuvent prendre la forme soit, d'un logiciel informatique soit, d'un support matériel. Dans le premier cas, il s'agit d'un processus furtif écrivant les informations captées dans un fichier caché. Dans le second cas, il s'agit alors d'un dispositif intercalé entre la prise clavier de l'ordinateur et le clavier.

1.4.6.4 Les vers :

Les vers tout comme les virus sont les deux exemples de logiciels malveillants les plus répandus et les plus connus. Ce sont des programmes malveillants capables de s'autorépliquer sur les ordinateurs ou via les réseaux informatiques et d'infecter les ordinateurs à l'insu de leurs utilisateurs. La plupart peuvent causer d'importants préjudices.

Dans la mesure où chaque copie du ver informatique peut à son tour s'autorépliquer, les infections peuvent se propager très rapidement. Il existe plusieurs catégories et sous-catégories de virus et vers informatiques. On peut citer les vers d'e-mail ou les vers de messagerie instantanée, les virus envoyés sous forme de pièces jointes ou via les réseaux de partages de fichier P2P.

La différence principale entre un virus et un vers est du fait que les virus nécessitent un programme hôte actif ou un système d'exploitation actif et déjà infecté pour s'exécuter, alors que les vers sont autonomes capables de s'autoreproduire et de se propager via les réseaux informatiques sans intervention humaine kaspersky [2020].

1.4.6.5 Les logiciels espions :

Encore appelés « Spyware » en anglais, ils correspondent à un terme générique désignant les logiciels espions qui s'introduisent dans un système informatique afin de recueillir à des fins commerciales le profil d'un utilisateur au regard de sa navigation sur le réseau Internet, voire le cas échéant obtenir des informations personnelles comme les références d'une carte bancaire, d'un permis de conduire ou tout autre document personnel et sensible.

Ces logiciels espions sont souvent inclus dans des logiciels gratuits et s'installent généralement à l'insu de l'utilisateur en même temps qu'il télécharge le logiciel en question. Ils sont souvent développés par des sociétés proposant de la publicité sur Internet. Pour permettre l'envoi ultérieur de publicité ciblée, il est nécessaire de bien connaître sa cible. Cette connaissance est grandement facilitée par ces logiciels espions kaspersky [2020].

1.4.6.6 Les botnets :

Contraction de robot et réseau, un « botnet » un terme générique qui désigne un groupe d'ordinateurs, de quelques milliers à plusieurs millions, contrôlés par un pirate à distance. Ce sont en réalité des programmes informatiques destinés à communiquer avec d'autres programmes similaires pour l'exécution de différentes tâches.

La plus connue consiste à prendre le contrôle à distance, en exploitant une faille de sécurité via un cheval de Troie ; par exemple, des milliers d'ordinateurs zombies forment un réseau de milliers de robots appelés communément des “botnets“.

Ces milliers d'ordinateurs contrôlés seront autant de relais pour permettre des attaques puissantes puisque les pirates pourront alors depuis leur domicile diffuser des codes malveillants tout en cachant leur identité. Les enquêteurs, dans le meilleur des cas, arriveront sur des ordinateurs dont les propriétaires sont également des victimes. Ces botnets représentent aujourd'hui une réelle menace pour notre société kaspersky [2020].

1.4.6.7 Ransomwares :

Un ransomware ou Rançongiciel en français est un type de logiciel malveillant, prenant en otage les données d'un individu ou d'une entreprise. Il est conçu pour extorquer de l'argent en bloquant l'accès aux fichiers ou au système informatique jusqu'à ce que la rançon soit payée. Les rançongiciels sont apparus pour la fois en Russie en 2005 kaspersky [2020] et se sont répandus dans le monde entier principalement aux Etats-Unis, en Australie ou en Allemagne. Généralement le Ransomware s'infiltre à travers un fichier téléchargé ou reçu par email et chiffre les données et fichiers de la victime. Une fois une machine infectée il est capable d'infecter les autres machines dans le même réseau d'où la nécessité de débrancher les machines infectées de rançongiciels du réseau de l'entreprise. Le paiement de la rançon ne garantit pas forcement que les fichiers seront récupérés. On distingue deux principales formes de ransomware :

Le ransomware Locker : ce type de ransomware verrouille l'accès et vous empêche d'utiliser les fonctionnalités de base de votre ordinateur. En général vous serez encore en mesure d'interagir avec la demande de rançon afin de procéder au paiement, mais votre ordinateur vous sera inutile pour toutes les autres fonctionnalités. Ce type de ransomware est moins dangereux car il n'affecte par les fichiers critiques de votre ordinateur.

Le ransomware crypto : ce type de ransomware chiffre vos données critiques (documents, images, vidéos), provoquant la panique chez leurs victimes. Ils n'affectent pas les fonctionnalités de base de l'ordinateur mais vos fichiers critiques, vos fichiers seront visibles et cryptés vous limitant ainsi l'accès. Les attaquants utilisant ce type de ransomware ont tendance à lancer un compte à rebours à leur demande de rançon menaçant leurs victimes de supprimer les fichiers après une certaine date ce qui le rend plus dangereux.
Les exemples courants de ransomwares sont : locky, Wannacry, Bad Rabbit, Rhuk etc...

1.5 Les services et mécanismes de sécurité :

Un service de sécurité est un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité **?** .Un mécanisme de sécurité est un mécanisme qui est conçu pour détecter, prévenir et lutter contre une attaque informatique.
Quelques bonnes pratiques pour améliorer la sécurité des systèmes informatiques :

1.5.1 Audit de sécurité :

L'audit de sécurité est l'identification des points de vulnérabilité d'un système. Il ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu. L'audit de sécurité est généralement assuré par un expert de la sécurité informatique au sein de l'entreprise.

Il conçoit les mécanismes de sécurité et attaques le système informatique de l'entreprise pour tester sa robustesse.

1.5.2 Journalisation (logs) :

La journalisation est l'enregistrement des activités de chaque acteurs (les utilisateurs). Il permet de constater que des attaques ont eu lieu, de les analyser et ainsi que de faire en sorte qu'elles ne se reproduisent pas.

1.5.3 Antivirus :

Les antivirus sont des logiciels dont le rôle est de protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables dangereux) néfastes. Il ne protège pas le réseau contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.

1.5.4 Utilisation de VPN :

Un VPN (Virtual Private Network) est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Un VPN permet de créer une liaison virtuelle entre deux noeuds physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante les données soient illisibles.

1.5.5 Systèmes de détection d'intrusion (IDS) :

Un systèmes de détection d'intrusion (IDS) comme son nom l'indique c'est un système mis en œuvre pour détecter les intrusion dans un ordinateur ou dans un réseau. Il existe depuis 1980 Bruneau [2020] et fait référence à tous les processus utilisés pour découvrir les utilisations non autorisées du réseau ou des objets du réseau . Ceci est réalisé grâce à un logiciel spécialement conçu dans le seul but de détecter une activité inhabituelle ou anormale.

Les systèmes de détection d'intrusion peuvent être classés en deux catégories Elike Hodo [2016] :

IDS basés sur l'hôte(HIDS) : Ce sont des logiciels produits installés sur un ordinateur hôte pour analyser et surveiller toutes les activités de trafic sur l'application système

IDS basés sur le réseau (NIDS) : Ceux-ci se trouvent sur un l'ensemble du réseau pour capturer et analyser le flux de paquets qui y transitent dans le réseau.

1.5.6 Les pare feu :

Un pare-feu (logiciel ou matériel) du réseau dont le rôle est de contrôler les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. Il n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système et ne protège pas le réseau contre une attaque venant du réseau intérieur (qui ne le traverse pas).

1.5.7 La reprise après sinistre et la continuité des activités :

La reprise après sinistre et la continuité des activités définissent la façon dont une organisation réagit à un incident de cybersécurité ou à tout autre événement entraînant la perte d'opérations ou de données. Les politiques de reprise après sinistre dictent la manière dont l'organisation restaure ses opérations et ses informations pour retrouver la même capacité opérationnelle qu'avant l'événement. La continuité des activités est le plan sur lequel l'organisation s'appuie tout en essayant de fonctionner sans certaines ressources.

1.5.8 La formation des utilisateurs finaux :

Aborde la formation du personnel de l'entreprise sur les notions de sécurité information vu le facteur humain constitue la plus grande vulnérabilité en termes de sécurité informatique. N'importe qui peut accidentellement introduire un virus dans un système par ailleurs sécurisé en ne respectant pas les bonnes pratiques de sécurité. En général les entreprises mettent en places des politiques de sécurités qui contiennent ces bonnes pratiques de sécurité :

- Apprendre aux utilisateurs à supprimer les pièces jointes suspectes,
- Ne pas brancher les clés USB non identifiées,
- Utilisation de mot de passe fort respectant les normes de sécurités,
- Une bonne maintenance du système informatique,
- Désignation d'un responsable de sécurité,
- La mise en place d'une politique de sauvegarde (back up) adaptée et redondante etc.

1.6 Conclusion :

Dans ce chapitre nous avons défini et décrit les différents aspects de la cybersécurité. La cybersécurité est un domaine très vaste et devient de plus en plus complexes à cause de la nature constante d'évolution des risques de sécurité et la complexité des systèmes informatique. Avec un nombre accru de points d'entrée pour les attaques, davantage de stratégies de sécurisation des actifs numériques sont nécessaires pour protéger les systèmes information. L'un des éléments les plus problématiques de la cybersécurité est de la veille technologique, Suivre les changements et les progrès continus des attaques et mettre à jour les pratiques pour les protéger contre les vulnérabilités potentielles.

Chapitre 2

INTERNET DES OBJETS

Sommaire

2.1 Introduction

Le concept d'Internet des Objets (IoT pour Internet of Things en anglais) a été proposé en 1999 par le laboratoire Auto-ID du Massachusetts Institute of Technology (MIT) Hu [2016]. Imaginez un monde où des milliards d'objets peuvent détecter, communiquer et partager des informations, tous interconnectés via des réseaux IP (Internet Protocol) publics ou privés. Ces objets interconnectés ont des données régulièrement collectées, analysées et utilisées pour initier l'action, fournissant une richesse d'intelligence pour la planification, la gestion et la prise de décision Patel u. a. [2016]. C'est le monde de l'Internet des objets (IoT).

Un exemple de base de tels objets comprend les thermostats et les systèmes de surveillance et de contrôle HVAC (chauffage, ventilation, climatisation) qui forment les composants des maisons intelligentes. Il existe également d'autre domaines et environnements dans lesquels l'IoT peut jouer un rôle remarquable et améliorer la qualité de nos vies. Ces applications comprennent soins de santé, transports, automatisation industrielle et réponse d'urgence aux catastrophes naturelles et d'origine humaine dont la prise de décision humaine est difficile.

L'idée de base de ce concept d'IoT est la présence omniprésente autour de nous d'une variété de choses ou d'objets - tels que des réseaux Wi-Fi, des réseaux cellulaires, des étiquettes d'identification par radiofréquence (RFID pour Radio Frequency Identification), des capteurs, des actionneurs, des téléphones mobiles, etc. - qui, grâce à des schémas d'adressage uniques, sont capables interagir entre eux et coopérer avec leurs voisins pour atteindre des objectifs communs Atzori u. a. [2010].

Dans ce chapitre, nous présentons l'Internet des Objets, l'origine de son concept, ses caractéristiques diverses. Puis on illustre ses différentes architectures, ses domaines d'application où il introduit de l'intelligence, ainsi que les enjeux et les défis que l'on peut rencontrer aux objets connectés.

2.2 Historique

Le premier « objet » connecté à l'Internet à utiliser ce nouveau protocole a été un grille-pain. En 1990, John Romkey, ingénieur logiciel et premier évangéliste d'Internet, en avait construit un qui pourrait être allumé et éteint sur Internet. Romkey a laissé tomber quelques tranches de pain dans le grille-pain et, à l'aide d'un ordinateur maladroit, a allumé le grille-pain. Il faudra encore une décennie avant que quiconque utilise l'expression « Internet des objets », mais le petit grille-pain magique de Romkey montre à quoi pourrait ressembler un monde d'objets connectés à Internet Pardes [2020].

Le terme « Internet of Things » lui-même a été inventé en 1999 dans le laboratoire Auto-ID du MIT lorsque le britannique Kevin Ashton (pionnier de la technologie) l'a mis dans une présentation pour l'entreprise Procter & Gamble. Le terme « Auto-ID » fait référence à toute grande classe de technologies d'identification utilisées dans l'industrie pour automatiser, réduire les erreurs et augmenter l'efficacité. Ces technologies comprennent les codes à barres, les cartes à puce, les capteurs, la reconnaissance vocale et la biométrie Sundmaeker u. a. [2010]. Ashton, qui travaillait alors dans l'optimisation de la chaîne d'approvisionnement, a remarqué que l'optimisation dépend directement de la vitesse de transmission et de traitement des données. Cela peut prendre des jours pour les personnes qui collectent les données. De plus, confier la tâche à des ordinateurs n'était pas envisageable car dépourvus d'organes sensoriels, ils étaient dépendants des informations

que des opérateurs humains voulaient bien leur fournir. L'utilisation de l'identification par radiofréquence (RFID) a permis d'accélérer le processus de transfert de données directement entre les appareils. Il avait une idée des choses à collecter, traiter et transmettre sans intervention humaine.

Alors qu'à domicile l'internet est devenu omniprésent et que le Wi-Fi s'est accéléré, le rêve de la maison intelligente a commencé à ressembler davantage à une réalité. Les entreprises ont commencé à présenter de plus en plus de ces inventions : des cafetières « intelligentes », des fours qui préparent des biscuits avec un minutage précis et des réfrigérateurs qui ont automatiquement réapprovisionné le lait périmé. Le premier d'entre eux, le réfrigérateur connecté à Internet de LG, a été lancé sur le marché en 2000. Il pourrait faire le point sur le contenu des étagères, et les dates d'expiration.

Internet des objets au fil des années	
1990	John Romkey crée le premier appareil IoT : un grille-pain qu'il contrôle avec son ordinateur
1999	Kevin Ashton invente le terme « Internet des objets » pour décrire un système où Internet est connecté au monde physique via des capteurs omniprésents
2000	LG présente son premier réfrigérateur connecté avec un prix de 20 000 $
2008	La première conférence Internet des Objets au monde se tient à Zurich, en Suisse
2010	Tony Fadell fonde Nest, qui développe des appareils électroménagers intelligents et des systèmes de gestion des bâtiments.
2013	Oxford Dictionary ajoute le terme « Internet of Things »
2014	Amazon présente le haut-parleur Echo, ainsi que l'assistant vocal Alexa, une nouvelle façon de contrôler la maison intelligente
2016	Un logiciel malveillant appelé Mirai a exploité des vulnérabilités dans plus de 600000 appareils IoT pour créer une attaque massive par déni de service distribué (**DDoS**).
2020	Selon certaines estimations, le nombre d'appareils connectés à Internet dépasse 20 milliards. Et les prévisions suggèrent que d'ici 2030, environ 50 milliards de ces appareils IoT seront utilisés dans le monde Department [2020].

TABLEAU 2.1 – Internet des Objets au fil des années

2.3 Définition

Le Cluster des projets européens de recherche sur l'Internet des objets (CERP-IoT pour Cluster of European Research Projects on the Internet of Things) définit l'Internet des objets comme : « une infrastructure dynamique d'un réseau global. Ce réseau global a des capacités d'auto-configuration basée sur des standards et des protocoles de communication interopérables. Dans ce réseau, les objets physiques et virtuels ont des identités, des attributs physiques, des personnalités virtuelles et des interfaces intelligentes, et ils sont intégrés au réseau d'une façon transparente » Sundmaeker u. a. [2010].
Cette vision de l'Internet des objets introduira une nouvelle dimension aux technologies de l'information et de la communication : en plus des deux dimensions temporelle et spatiale qui permettent aux personnes de se connecter de n'importe où à n'importe quel moment, nous aurons une nouvelle dimension « objet » qui leur permettra de se connecter à n'importe quel objet Challal [2012] (Smartphone, tablettes, capteurs, caméras de vidéo-surveillance, etc.). Un objet connecté a une valeur lorsqu'il est connecté à d'autres objets et consorts logiciels, par exemple : une montre connectée n'a d'intérêt qu'au sein d'un écosystème orienté santé/bien-être, qui va bien au-delà de connaître l'heure.

L'Internet des Objets a pour but de permettre aux objets d'être connecté à tout moment, en tout lieu, avec n'importe quoi et n'importe qui en utilisant n'importe quel chemin / réseau et n'importe quel service Patel u. a. [2016].

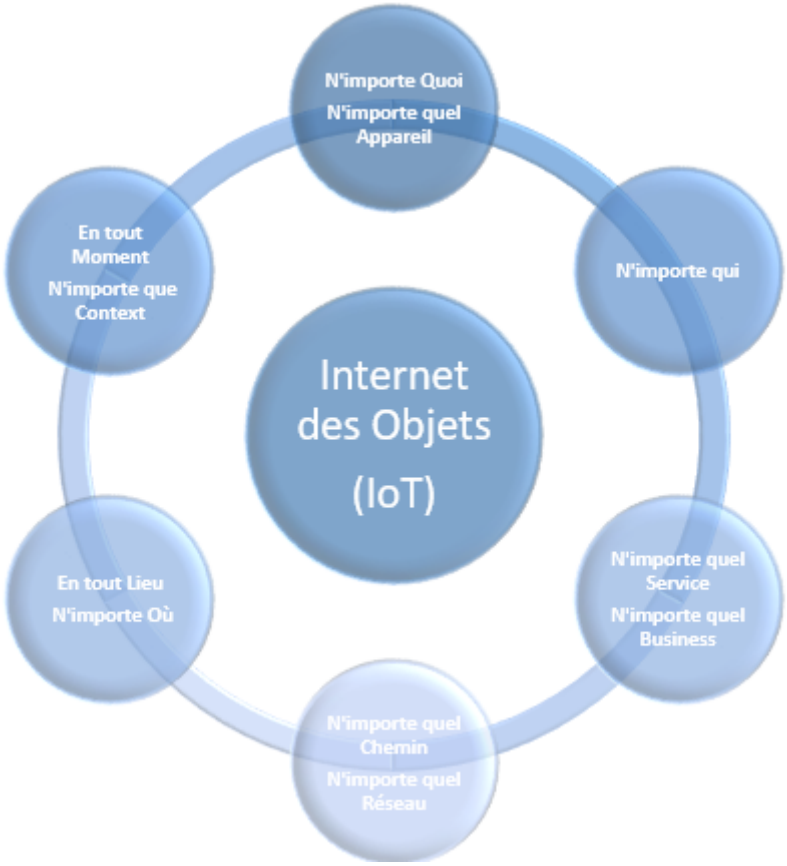

FIGURE 2.1 – Internet des Objets

L'Internet des Objets peut être défini également comme « des données et des appareils

disponibles en permanence à travers l'internet » Hu [2016].

Un objet connecté est un objet possédant la capacité d'échanger des données avec d'autres entités physiques ou numériques.

À peu près n'importe quel objet physique peut être transformé en un appareil IoT s'il peut être connecté à Internet pour être contrôlé ou communiquer des informations avec le réseau indépendamment de l'action humaine.

Pour illustrer, prenons un exemple dans le domaine de l'habitat intelligent, aussi connu sous le nom de Smart Home. Imaginez que votre réfrigérateur devienne intelligent. Un réfrigérateur capable de vous dire en temps réel le type de denrées qu'il y a à l'intérieur et capable de passer commande pour vous quand vous avez besoin de vous réapprovisionner.

Le réfrigérateur est un exemple typique mais le nombre d'objets qu'il est aujourd'hui possible de connecter pour s'échanger des données est illimité.

FIGURE 2.2 – Internet des Objets

2.4 Caractéristiques

Les caractéristiques fondamentales de l'IoT sont les suivantes Patel u. a. [2016]; Vermesan u. a. [2014] : **Inter connectivité** : en ce qui concerne l'IoT, tout peut être interconnecté avec l'infrastructure mondiale d'information et de communication.

Services liés aux objets : l'IoT est capable de fournir des services liés aux objets dans les limites des objets, tels que la protection de la vie privée et la cohérence sémantique entre les objets physiques et les objets virtuels associés. Afin de fournir des services liés aux objets dans les contraintes des objets, les technologies du monde physique et du monde de l'information vont changer.

Hétérogénéité : les appareils de l'IoT sont hétérogènes car basés sur différentes plates-formes matérielles et réseaux. Ils peuvent interagir avec d'autres appareils ou plates-formes de services via différents réseaux.

Changements dynamiques : l'état des appareils change de manière dynamique, par exemple, le sommeil et le réveil, connectés et / ou déconnectés ainsi que le contexte des appareils, y compris l'emplacement et la vitesse. De plus, le nombre d'appareils peut changer dynamiquement.

Échelle énorme : le nombre d'appareils qui doivent être gérés et qui communiquent entre eux sera au moins d'un ordre de grandeur supérieur à celui des appareils connectés à l'Internet actuel. Encore plus critique sera la gestion des données générées et leur interprétation à des fins d'application. Cela concerne la sémantique des données, ainsi que la gestion efficace des données.

Sécurité : à mesure que nous tirons parti de l'IoT, nous ne devons pas oublier la sécurité. En tant que créateurs et destinataires de l'IoT, nous devons concevoir pour la sécurité. Cela comprend la sécurité de nos données personnelles et la sécurité de notre bien-être physique. Sécuriser les points de terminaison, les réseaux et les données se déplaçant sur tout cela signifie créer un paradigme de sécurité qui évoluera.

Intelligence : L'IoT est livré avec la combinaison d'algorithmes et de calcul, de logiciels et de matériel qui le rendent intelligent. Ce qui le rend encore plus intelligent, ce sont les données qu'il recueille à travers un capteur. L'intelligence ambiante dans l'IoT améliore ses capacités qui facilitent les choses pour répondre de manière intelligente à une situation particulière et les aide à effectuer des tâches spécifiques. Malgré toute la popularité des technologies intelligentes, l'intelligence dans l'IoT ne concerne que les moyens d'interaction entre les appareils, tandis que l'interaction utilisateur et appareil est obtenue par des méthodes d'entrée standard et une interface utilisateur graphique.

Connectivité : la connectivité permet l'accessibilité et la compatibilité du réseau. L'accessibilité se fait sur un réseau tandis que la compatibilité offre la capacité commune de consommer et de produire des données.

2.5 Architecture de l'IoT

L'IoT devrait être capable d'interconnecter des milliards d'objets hétérogènes via le réseau internet, ainsi il est judicieux d'adopter une architecture flexible. Le modèle de base est une architecture à trois-couches comportant les couches Application, Réseau, et Perception. D'autres modèles ont été proposé récemment qui ajoutent plus d'abstraction aux architectures des objets connectés. La figure ci-dessous illustre les différentes catégories de l'architecture IoT Al-Fuqaha u. a. [2015].

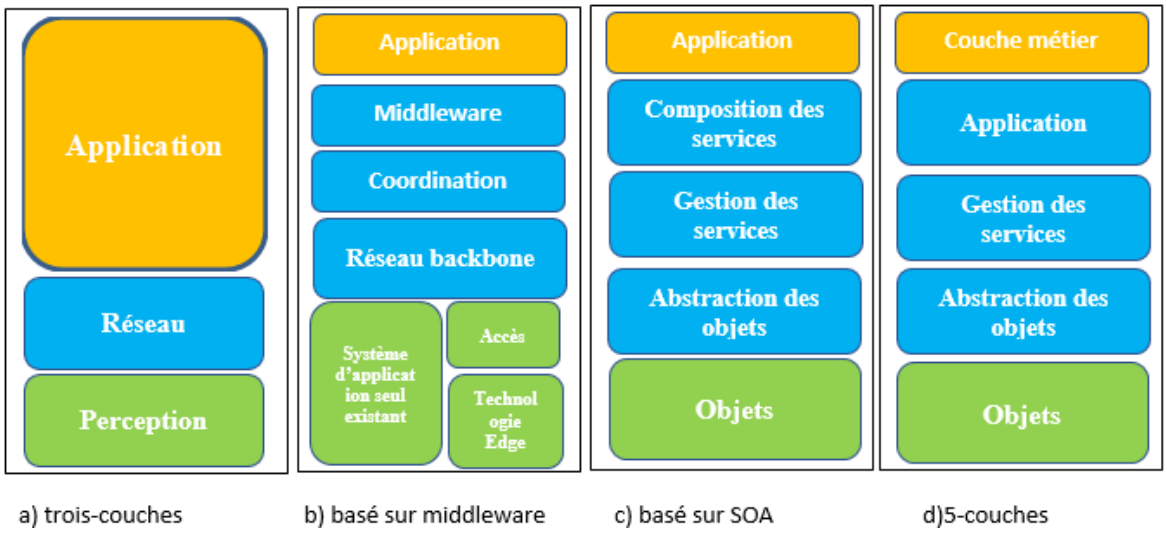

FIGURE 2.3 – Diverses architectures de l'IoT

2.5.1 Architecture à trois couches

2.5.1.1 Couche perception

La première couche de l'IoT, les Objets (appareils) ou couche perception, est un organe sensoriel de l'IoT, représente les capteurs physiques de l'IoT qui essaie de recueillir et traiter les données. Un capteur de température permet de traduire l'amplitude de la température en une tension électrique. Cette couche comprend principalement des éléments avec des étiquettes RFID, capteurs, et autre terminaux. Elle détecte les données de l'environnement. Certains facteurs sont pris en charge par la couche physique tels que : ressource, hétérogénéité, déploiement, protocoles.

2.5.1.2 Couche réseau

La couche réseau est chargée de récupérer les données collectées du capteur. L'échange des données se fait via cette couche. Ainsi, la couche réseau peut agréger les données dans sa propre base de données ou un stockage cloud.

2.5.1.3 Couche application

La couche application ou la couche interface utilisateur contient les méthodes d'interaction avec les applications de l'utilisateur.

2.5.2 Architecture à cinq couches

2.5.2.1 Couche Objets

La première couche de l'IoT, les Objets (appareils) ou couche perception, représente les capteurs physiques de l'IoT qui essaie de recueillir et traiter les données. Cette couche comprend les capteurs et les actionneurs qui fonctionnent différemment. Un capteur de température permet de traduire l'amplitude de la température en une tension électrique. On a d'autres grandeur mesurable tels que pression, luminosité, position, vitesse. Quant aux actionneurs, ils permettent d'agir dans le monde physique en changeant son état. Un actionneur peut allumer un appareil à distance. La couche perception collecte les informations du capteur, numérise et transmet les données à la couche Abstraction Objet via un canal sécurisé.

2.5.2.2 Couche Abstraction Objet

La couche Abstraction Objet transfert les données produit par la couche perception à la couche Gestion Service à travers des canaux sécurisés. Les données peuvent être transféré via des technologies variés tels que RFID, GSM(2G), UMTS(3G), LTE(4G), WI-FI, Bluetooth, Zigbee, etc. En plus, d'autres fonctions comme Cloud Computing et le traitement de gestion de données sont gérés par cette couche.

2.5.2.3 Couche Gestion des Services

La couche Gestion des Services garantit la fourniture des services en fonction de la demande de l'utilisateur dans un environnement réseau hétérogène.

2.5.2.4 Couche Application

La couche Application fournit les services demandés par les clients. Par exemple, la couche application peut fournir les mesures de température au client qui demande cette information. Elle couvre différentes applications, à savoir : ville intelligente, transport intelligent, soins de santé, agriculture intelligente, maison intelligente, etc.

2.5.2.5 Couche Business

La couche métier(gestion) est chargée de gérer l'ensemble des activités et des services comme les modèles métiers. Elle aide à construire un graphique, un organigramme, un modèle métier, une prise de décision etc. basé sur les données reçues de la couche Application.

2.6 Domaines d'application

Il existe une panoplie de domaines d'application extrêmement diverses pour les secteurs de l'internet des objets, du machine to machine et des objets connectés. Parmi ces principaux domaines, nous citons : la smart city, la domotique, les transports, la santé, l'industrie, l'agriculture.

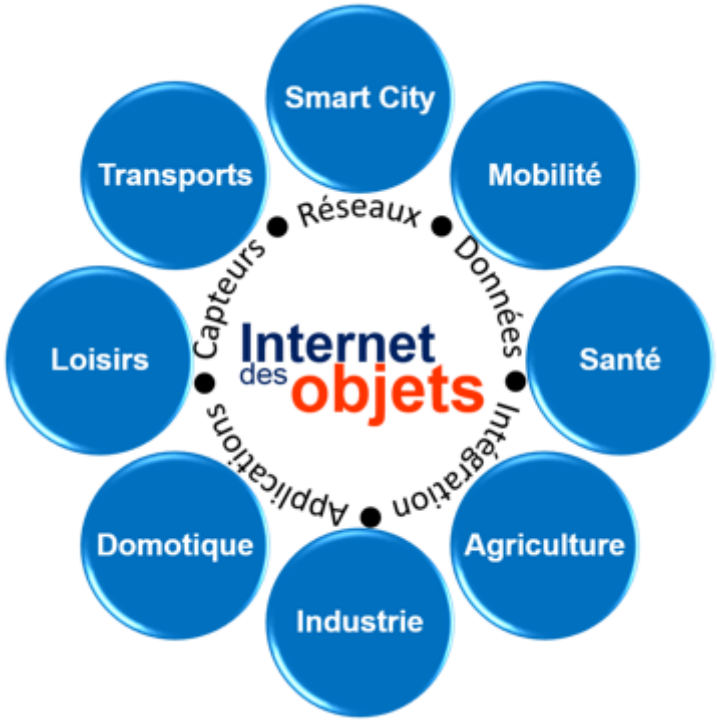

FIGURE 2.4 – Domaines d'application de l'IoT

1. **Smart city** Dans les villes intelligentes, il améliore la qualité de vie des habitants en utilisant les nouvelles technologies pour accroître l'efficacité des services, optimiser l'éclairage, de maîtriser la consommation d'énergie et de réduire l'impact écologique des activités urbaines.
2. **Domotique** La domotique regroupe l'ensemble des technologies permettant l'automatisation des équipements d'un habitat. Elle vise à apporter des solutions techniques pour répondre aux besoins de confort (gestion d'énergie, optimisation de l'éclairage et du chauffage), de sécurité(alarme) et de communication (commandes à distance) Locqueneux [2015]. La domotique couvre trois domaines principaux :
   (a) Confort de la vie quotidienne : l'IoT permettra aux propriétaires de villa de déclencher arrosage, fermeture des fenêtres ou tonte du gazon en fonction des informations transmises par les capteurs disposés dans le jardin.
   (b) Assurer la protection des personnes et des biens par la prévention des risques d'accident (incendies, fuite de gaz, etc.).
   (c) Faciliter les économies d'énergie grâce à la réaction maitrisée d'une maison intelligente.
3. **Santé** Dans le domaine de la santé, l'internet des objets offrira une sécurité accrue à un patient dont un capteur est intégré sur le corps qui donne la possibilité d'être monitoré à distance. Il peut informer un patient quand il est temps de prendre le médicament. En outre, cela pourrait éventuellement informer le médecin d'une situation d'urgence lui permettant ainsi de localiser le patient grâce à l'objet connecté.
4. **Transport** Des voitures connectées ou autonomes aux systèmes de transports intelligents, l'IoT pourra sauver des vies, réduire le trafic et minimiser l'impact des véhicules sur l'environnement.

5. **Industrie** Dans le secteur industriel, le machine to machine peut augmenter énormément la productivité et la performance d'une usine. Par exemple, supposons un réseau de capteurs polyvalents qui suit à distance et pilote le fonctionnement des machines en leur donnant la possibilité de déclencher elles-mêmes un réapprovisionnement en matières premières.
6. **Agriculture** L'internet des objets à un impact énorme sur le domaine de l'agriculture. Les éleveurs en bénéficient en effectuant un suivi plus précis de l'alimentation, de la santé et de la sécurité du bétail. Ils peuvent aussi géolocaliser leur bétail en temps réel. Les agriculteurs peuvent aussi recueillir des données sur les engrais et les pesticides nécessaires à leurs cultures Krigman [2018].

2.7 Enjeux et défis de l'IoT

L'internet des objets soulève un nombre important de questions, mais le plus important porte certainement sur la sécurité. Beaucoup de produit connectés, dont certains que nous utilisons au quotidien affichent un réel manque de maturité impliquant de nouvelles préoccupation notamment autour de la confidentialité et la sécurité des données. Mirai est un exemple type de cyberattaques résultant de menaces de sécurité liées à l'IoT.

Enjeux	**Défis**
Architecture	De nombreux chercheurs ont proposé diverses architectures non encore standardisé.
Sécurité	L'échange d'information entre des milliards d'objets connecté sur internet se fait via une connexion réseau sans fil.
Confidentialité	Les opérations d'accès aux profils entre objets sans interférences sont difficiles.
Intéroperabilité	Communication machine à machine (M2M), un défi de l'IoT dû à la nécessité de gérer un grand nombre d'objets hétérogènes qui appartiennent à différentes plates-formes.
Disponibilité	La capacité à fournir des services à tout moment, n'importe où et n'importe quoi est un défis.
Mobilité	L'utilisateur ou les appareils qui se connectent peuvent obtenir les services lors de leurs déplacements, ce qui constitue un défi.
Scalabilité	La possibilité d'ajouter de nouveaux appareils qui n'affecte pas la qualité de services existent est un défi.

TABLEAU 2.2 – Enjeux et défis de l'IoT

2.8 Sécurité, confidentialité (privacy) en IoT

L'IoT nécessite cinq phases, de la collecte des données, du stockage, du traitement, de la transmission des données à la livraison des données aux utilisateurs finaux sur demande ou non Hu [2016]. Les capteurs collectent dans de nombreux cas des données extrêmement sensible (personnelles). En effet les objets connectés produisent de grandes quantités de données à la phase de collecte de données et le traitement de cette masse de données implique de nouvelles préoccupations notamment autour de la confidentialité et la sécurité des données.

FIGURE 2.5 – Défis de sécurité IoT

2.8.1 Sécurité pour l'IoT

La sécurité est l'affaire de tous, elle concerne chacun de nous. Si vous achetez un verrou « intelligent » pour votre porte d'entrée, il est fort probable que vous allez vous faire pirater dans un premier temps puis cambrioler. L'IoT a des avantages et apporte tous celui d'internet à des éléments comme les thermostats et les ampoules par exemple mais sans oublier qu'il apporte également les problèmes d'internet. A présent que les gens ont leur réfrigérateurs, sonnettes, télévisions, ampoules, caméras de sécurité, haut-parleur connectés au Wi-Fi, presque tous les appareils de la maison peuvent être compromis ou rendu inutiles. En effet les objets connectés peuvent servir de point d'accès à votre réseau avec vos portables, votre PC, bref toute votre vie.

La menace qui pèse sur les appareils connectés à Internet ne vient pas uniquement du fait qu'ils sont connectés à Internet, mais aussi parce que les fabricants d'appareils n'ont pas toujours conçu leurs produits en privilégiant la sécurité. À mesure que l'IoT se répand largement, les cyberattaques risquent de devenir de plus en plus physiques (et pas simplement virtuelles) **?**. Les appareils contrôlés par ordinateur dans les automobiles, tels que les freins, les moteurs, les serrures, les klaxons, les systèmes de chauffage et les tableaux de bord, se sont révélés vulnérables aux attaquants qui ont accès au réseau de bord **??**. La possibilité qu'un intrus puisse démarrer à distance le chauffage, régler le climatiseur, déverrouiller les portes, déployer des airbags pendant que vous conduisez sans accident ou tourner le volant d'une voiture en marche est en effet inquiétante, effrayante.

Jusque-là l'essentiel des dommages subit par l'IoT a été causé par les botnets. En septembre 2016, une attaque a été mis en place par des centaines de milliers d'objets connecté piraté pour former un énorme botnet appelé Mirai. Ce malware a exploité des vulnérabilités (que les fabricants d'objet connecté ne prenaient pas en compte) dans plus de 600

000 appareils IoT pour créer une attaque massive par déni de service distribué (**DDoS**). Il avait pour objectif de dénoncer les risques de l'IoT.

En raison de la vulnérabilité du WPA2(protocole qui sécurise les échanges en Wi-Fi), tout ce qui est connecté à un réseau Wi-Fi risque d'être piraté **?**. L'année suivante après Mirai, une attaque appelée KRACK acronyme de Key Reinstallation Attack (attaque de réinstallation de clé) a infecté presque tous les appareils connectés à Internet connectés au Wi-Fi. L'attaque était paralysante et difficile à résister, en partie parce que l'Internet des objets fonctionne sur de nombreux systèmes d'exploitation essentiellement différent. Lorsqu'un téléphone ou un ordinateur est touché par un virus, les fabricants de logiciels sont généralement prompts à émettre un correctif. Mais des choses comme les routeurs ou les sonnettes connectées à Internet ne sont pas mis à jour aussi régulièrement que les systèmes d'exploitation informatique pour se protéger contre les vulnérabilités, et beaucoup d'entre elles n'ont pas été construites avec le même type de protocoles de sécurité que les ordinateurs Pardes [2020]. C'est une réalité, l'IoT nous rend encore plus connecter et cette connexion de tous les instants vient avec son l'eau de risque qu'on ne peut pas ignorer. Les menaces virtuelles vont s'immiscer dans le monde physique, ce qui signifie que le piratage des appareils peut avoir des conséquences dangereuses dans le monde réel.

L'IoT n'est pas encore arrivé à maturité et est extrêmement vulnérable à toutes sortes de menaces et d'attaques ou vol de données. Les systèmes de prévention ou de récupération utilisés dans le réseau traditionnel et Internet ne peuvent pas être utilisés dans l'IoT en raison de sa connectivité Hu [2016]. Les raisons de sa vulnérabilité sont multiples Atzori u. a. [2010]. Primo, souvent ses composants passent la plupart du temps sans surveillance ; et ainsi, il est facile de les attaquer physiquement. Secundo, la plupart des communications sont sans fil, ce qui rend l'écoute extrêmement simple. Enfin, la plupart des composants IoT sont caractérisés par de faibles capacités en termes à la fois d'énergie et de ressources informatiques (c'est particulièrement le cas pour les composants passifs) et, par conséquent, ils ne peuvent pas mettre en œuvre des schémas complexes prenant en charge la sécurité.

La sécurité des informations et du réseau doit être dotée de propriétés telles que, la confidentialité, l'intégrité, l'identification et la disponibilité. Plus précisément, les problèmes majeurs de l'IoT liés à la sécurité concernent l'*authentification* et l'*intégrité des données* Atzori u. a. [2010] :

- L'authentification est requise pour établir une connexion entre les appareils et l'échange de nombre de clés publiques et privées via le nœud pour empêcher le vol de données. L'authentification est difficile car elle nécessite généralement des infrastructures d'authentification et des serveurs appropriés qui atteignent leur objectif grâce à l'échange de messages appropriés avec d'autres nœuds. Dans l'IoT, de telles approches ne sont pas réalisables étant donné que les étiquettes RFID passives ne peuvent pas échanger trop de messages avec les serveurs d'authentification. Le même raisonnement s'applique (de manière moins restrictive) aux nœuds de capteur également.
- Les solutions d'intégrité des données doivent garantir qu'un adversaire ne peut pas modifier les données de la transaction sans que le système détecte le changement. En d'autre terme, elles garantissent que les données qui sont arrivées au nœud récepteur sont inchangées et restent telles que transmises par la source (expéditeur). Un autre facteur critique qui influence l'intégrité des données est la robustesse et les capacités de tolérance aux pannes du système IoT. Les réseaux de capteurs, tels que les solutions RFID, sont également confrontés à d'autres problèmes qui limitent

leur capacité à surmonter les problèmes d'intégrité, car bon nombre de leurs composants passent la plupart du temps sans être pris en charge, sans surveillance **?**. Les données peuvent être modifiées par des attaquants pendant qu'elles sont stockées dans le nœud ou lorsqu'elles traversent le réseau **?**. Pour protéger les données contre ces types d'attaque, les protections en lecture et en écriture ainsi que les méthodes d'authentification sont généralement des solutions courantes à ces problèmes. Les ressources trouvées dans les systèmes IoT courants ne prennent pas en charge les techniques cryptographiques (permettant de stocker, traiter et partager des données protégées sans que le contenu de l'information soit accessible à d'autres parties) typiques en raison des ressources limitées disponibles **?**. L'intégrité de l'Internet des objets doit non seulement être protégée des sources externes mais également des processus internes, tels que l'intégrité des services.

2.8.2 Confidentialité pour l'IoT

Il y a ensuite la question de la confidentialité. La confidentialité des données est une condition pour que les données ne soient disponibles que pour les utilisateurs autorisés. Elle consiste à garder les données privées plutôt que de les autoriser à être disponibles dans le domaine public.

L'IoT représente un environnement dans lequel la vie privée des individus est fortement menacée. Si des caméras et des microphones sont installés autour de votre maison, ils vous regardent et vous écoutent. Tout dans l'internet des objets collecte des données et toutes ces données sont d'une valeur inestimable. Ainsi, lorsque les entreprises gagneront de l'argent en vous vendant des objets connectés intelligents en premier lieu, leur modèle commercial IoT implique probablement la vente d'au moins certaines de ces données également.

Ce qui arrive à ces données est une question de confidentialité d'une importance vitale. Toutes les entreprises de maisons intelligentes ne construisent pas leur modèle commercial autour de la collecte et de la vente de vos données, mais certaines le font **?**.

De nombreux appareils de dernière génération dans nos maisons sont équipés d'une connectivité qui permet une grande commodité, mais cet avantage a un prix (des risques potentiels d'espionnage et de sécurité). En janvier 2014, Forbes a répertorié de nombreux appareils connectés à Internet tels que des téléviseurs, des appareils de cuisine, des modems(et ISP), des, des caméras, des thermostats(chauffage et climatisation), et des équipements de buanderie qui peuvent déjà « espionner des personnes dans leur propre maison » **?**. Cela signifie que les détails les plus fins de votre vie personnelle, tels que exposés par votre réfrigérateur intelligent, votre télévision intelligent ou votre haut-parleur intelligent, peuvent être recueillis et vendus à quelqu'un d'autre ou pour faire du chantage. Google et Apple ont tous deux admis, l'an dernier, que les enregistrements capturés par leurs haut-parleurs intelligents étaient examinés par des entrepreneurs, y compris des extraits audio maladroits et intimes.

La sécurisation des échanges de données est nécessaire pour éviter de perdre ou de compromettre la confidentialité.

2.9 Conclusion

L'IoT est un concept en évolution constante dont l'objectif est d'étendre le réseau internet en interconnectant les objets connectés, ainsi effectué des échanges de données aux

objets du monde physique. Ces objets connectés à internet peuvent prendre la forme de n'importe quel objet du quotidien.

Il existe plusieurs architectures de l'IoT tels que l'architecture basé trois-couches, basé sur middleware, basé sur SOA et basé cinq-couches. Tout appareil connecté à Internet présente un risque élevé, et les appareils IoT ne font pas exception. L'IoT peut être vu comme « Interconnections of Threats » c'est-à-dire interconnexions des menaces dû à l'extension du réseau internet. La sécurité et la confidentialité des données sont de grands défis dans l'IoT. Lors de la transmission transparente des données, il est important de se cacher des appareils d'observation sur Internet qui sont susceptibles de nous espionner.

Deuxième partie

Contributions

Chapitre 3

DEEP LEARNING : LES RÉSEAUX DE NEURONES

Sommaire

Sommaire

3.1 Introduction

3.2 Historique

3.3 Définition

3.4 Caractéristiques

Bibliographie

[Adat u. a. 2017] ADAT, V.; GUPTA, B. B.; YAMAGUCHI, S. : Risk transfer mechanism to defend DDoS attacks in IoT scenario. (2017), S. 37–40 3

[Al-Fuqaha u. a. 2015] AL-FUQAHA, Ala; GUIZANI, Mohsen; MOHAMMADI, Mehdi; ALEDHARI, Mohammed; AYYASH, Moussa : Internet of things : A survey on enabling technologies, protocols, and applications. In : *IEEE communications surveys & tutorials* 17 (2015), Nr. 4, S. 2347–2376 27

[Atzori u. a. 2010] ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo : The internet of things : A survey. In : *Computer networks* 54 (2010), Nr. 15, S. 2787–2805 22, 33

[Bruneau 2020] BRUNEAU, Guy : The History and Evolution of Intrusion Detection. In : *SANS Institute Information Security Reading Room* (2020), April. – URL https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344 19

[Buckley] BUCKLEY, Kaitlin : *Survey finds security continues to be top priority in deploying IoT projects*. – URL https://451research.com/blog/1934-survey-finds-security-continues-to-be-top-priority-in-deploying-iot-projects 1

[Challal 2012] CHALLAL, Yacine : *Sécurité de l'Internet des Objets : vers une approche cognitive et systémique*, Dissertation, 2012 24

[Dave 2011] DAVE, Evans : The Internet of Things How the Next Evolution of the Internet Is Changing Everything. In : *Cisco Internet Business Solutions Group (IBSG)* (2011), Avril 1

[Department 2020] DEPARTMENT, Statista R. : *Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030*. 2020. – URL https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/ 23

[Elike Hodo 2016] ELIKE HODO, Andrew H. : Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System. In : *Department of Electronic Electrical Engineering University of Strathclyde Glasgow G1 1XW UK* (2016), April. – URL https://arxiv.org/ftp/arxiv/papers/1704/1704.02286.pdf 19

[Hu 2016] HU, Fei : *Security and privacy in Internet of things (IoTs) : Models, Algorithms and Implementations*. CRC Press, 2016. – ISBN 978-1-4987-2319-0 22, 25, 31, 33

[infosec] INFOSEC : *Internet of Things : How Much are We Exposed to Cyber Threats?*. – URL https://resources.infosecinstitute.com/internet-things-much-exposed-cyber-threats/ 1, 2

[Jégo 2007] JÉGO, Marie : L'Estonie tire les leçons des cyberattaques massives lancées contre elle pendant la crise avec la Russie. In : *Journal Le Monde* (2007), juin. – URL https://www.lemonde.fr/europe/article/2007/06/27/l-estonie-tire-les-lecons-des-cyberattaques-massives-lancees-contre-elle-pendant-928568_3214.html 2

[kaspersky] KASPERSKY : *Internet des objets : qu'est-ce que l'IoT? IoT Security.* – URL https://www.kaspersky.fr/resource-center/definitions/what-is-iot 1

[kaspersky.] KASPERSKY. : *what-is-cyber-security.* – URL https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security.kaspersky.fr. 11, 13

[kaspersky 2020] KASPERSKY : *what-is-ransomware.* 2020. – URL https://www.kaspersky.fr/resource-center/definitions/what-is-ransomware. 14, 16, 17, 18

[Krigman 2018] KRIGMAN, A. : *Bétail connecté, contrôle des récoltes, drones... l'Internet des Objets transforme l'agriculture à grande vitesse.* 2018. – URL https://www.globalsign.fr/fr/blog/l-iot-ameliore-l-agriculture-avec-le-betail-connecte-et-les-drones/ 30

[Locqueneux 2015] LOCQUENEUX, Cédric : *La domotique, c'est quoi?* 2015. – URL https://www.maison-et-domotique.com/47895-la-domotique-cest-quoi/ 29

[MARWA 2016] MARWA, Ahmim : *Etude du protocole IPSEC et metriques de sécurité*, Université BADJI MOKHTAR ANNABA, Dissertation, 2016 12

[Muhammad Aamir1 2019] MUHAMMAD AAMIR1, Ali Z. : DDoS attack detection with feature engineering and machine learning :the framework and performance evaluation. In : *International Journal of Information Security* (2019), Avril, S. 2 14

[pandasecurity] PANDASECURITY : *types-de-cybercriminalite.* – URL https://www.pandasecurity.com/france/mediacenter/securite/types-de-cybercriminalite/ 13

[Pardes 2020] PARDES, Arielle : *The WIRED Guide to the Internet of Things.* 2020. – URL https://www.wired.com/story/wired-guide-internet-of-things/ 22, 33

[Patel u. a. 2016] PATEL, Keyur K. ; PATEL, Sunil M. u. a. : Internet of things-IOT : definition, characteristics, architecture, enabling technologies, application & future challenges. In : *International journal of engineering science and computing (IJESC)* 6 (2016), Nr. 5 22, 24, 26

[Perakovic u. a. 2015] PERAKOVIC, Dragan ; PERIŠA, Marko ; CVITIĆ, Ivan : Analysis of the IoT Impact on Volume of DDoS Attacks. (2015), 12, S. 1 3

[ROSE 2000] ROSE, Colin : *Discours prononcé lors de l'ouverture du G-8 sur la cybercriminalité, Paris.* 2000. – Discours 13

[futura sciences 2020] SCIENCES futura : *informatique-attaque-man-in-middle-10048.* 2020. – URL https://www.futura-sciences.com/tech/definitions/informatique-attaque-man-in-middle-10048/ 16

[Solange 2019] SOLANGE, Ghernaouti : *Cybersécurité Analyser les risques Mettre en œuvre les solutions.* DUNOD, 2019 11, 13

[statista 2020] STATISTA : *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025.* 2020. – URL https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ 1

[ssi.ac strasbourg.fr.] STRASBOURG.FR. ssi.ac : *lidentification-et-lauthentification*. – URL https://ssi.ac-strasbourg.fr/bonnes-pratiques/recommandations/lidentification-et-lauthentification/ 9

[Strawbridge] STRAWBRIDGE, Geraldine : 10 Biggest DDoS Attacks and how your organisation can learn from them. In : *metacompliance*. – URL https://www.metacompliance.com/blog/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them/ 2

[Sundmaeker u. a. 2010] SUNDMAEKER, Harald ; GUILLEMIN, Patrick ; FRIESS, Peter ; WOELFFLÉ, Sylvie : Vision and challenges for realising the Internet of Things. In : *Cluster of European Research Projects on the Internet of Things, European Commision* 3 (2010), Nr. 3, S. 34–36 22, 24

[Vermesan u. a. 2014] VERMESAN, Ovidiu ; FRIESS, Peter u. a. : *Internet of things-from research and innovation to market deployment*. Bd. 29. River publishers Aalborg, 2014 26

[Wiener 1948] WIENER, Norbert : *Cybernetics or Control and Communication in the Animal and the Machines*. 1948 11

[William 1984] WILLIAM, Gibson : *Neuromancer*. Ace, 1984 11

[Zhang Hang 2013] ZHANG HANG, Han M. : BUSINESS INTELLIGENCE ARCHITECTURE BASED ON INTERNET OF THINGS. In : *Journal of Theoretical and Applied Information Technology* (2013), April 1