Introduction à la cybersécurité des systèmes industriels

La Revue 3E.I
Culture Sciences de l'Ingénieur

Édité le 15/02/2024

école normale supérieure paris—saclay

Maxime SECHEHAYE[1], Anthony JUTON[2]

[1] *Etudiant en M2 à l'ENS Paris-Saclay – DER Nikola Tesla*

[2] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cette ressource introduit le dossier sur la cybersécurité en définissant ses objectifs, les principes fondamentaux de la cybersécurité ainsi que ses enjeux.

D'après le dictionnaire *Le Robert*, la cybersécurité désigne « l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, etc. ». Aborder la cybersécurité dans son ensemble est donc une tâche colossale qui nécessite des connaissances et des compétences dans de très nombreux domaines : économie, diplomatie, droit, sociologie, renseignement, etc. Se former en cybersécurité, ce n'est donc pas uniquement apprendre de bonnes pratiques en informatique, le champ d'application est bien plus vaste.

Cette ressource définit donc les limites de ce dossier qui ne se veut pas exhaustif, puis précise le public visé, avant de présenter quelques attaques récentes liées à des problématiques de cybersécurité pour commencer à sensibiliser le lecteur.

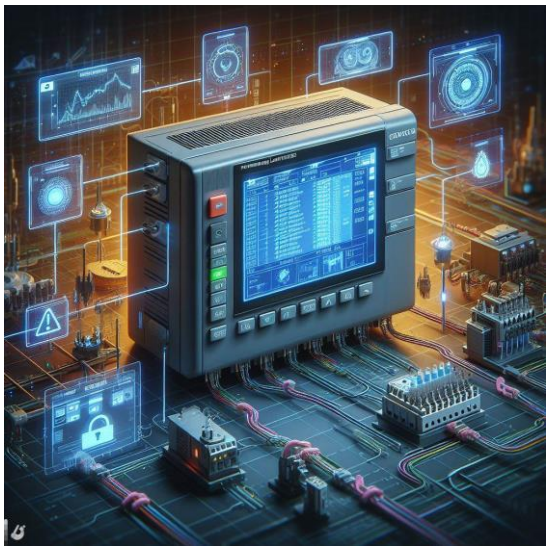


Figure 1 : Cybersécurité des systèmes automatisés industriels, vue par Microsoft Designer / DALL-E3

1 - Les champs de la cybersécurité couverts par ce dossier

Comme beaucoup des disciplines informatiques, la cybersécurité des systèmes informatiques est un sujet largement traité avec des ressources de qualité accessibles librement et destinées à des informaticiens.

La cybersécurité des systèmes industriels est à l'intersection entre la cybersécurité des systèmes informatiques et le champ disciplinaire nommé en France « informatique industrielle » qui regroupe l'automatisme industriel et l'informatique embarquée. Pour le premier, l'« industrie 4.0 » et pour le second, l'« internet des objets », sont deux expressions (aux contours peu précis) très utilisées qui traduisent la tendance à la « connexion de tout, toujours et partout ». Ceci élargit la surface vulnérable des systèmes industriels et amène à une augmentation du nombre des attaques. Ces systèmes, automatisés, embarqués ou IoT, ont de plus une durée de vie importante allant souvent au-delà de la période couverte par les mises à jour de sécurité (quand elles sont faites...).

Cela implique une meilleure formation des acteurs, notamment ceux issus de l'informatique industrielle, à la cybersécurité, d'où notamment l'évolution du BTS Systèmes Numériques en BTS Cybersécurité, Informatique et réseaux, Électronique (CIEL) et l'introduction de la cybersécurité dans le programme national des BUT GEII et R&T (pour lequel existe désormais un parcours cybersécurité).

Accompagnant ce mouvement, ce dossier vise à proposer aux enseignants d'informatique industrielle des ressources théoriques, des exemples de travaux pratiques et des témoignages d'industriels, organisés en trois domaines, pas complètement indépendants, après une partie introductive :

- Cybersécurité des systèmes automatisés industriels,
- Cybersécurité des objets connectés,
- Cybersécurité des systèmes embarqués (essentiellement automobiles).

Pour chacun de ces ensembles de systèmes, le dossier s'intéresse essentiellement aux vulnérabilités et protections au niveau réseau, en restant dans le cadre des compétences attendues d'un technicien ou ingénieur en GEII.

En complément, une dernière partie présentera une introduction à la cybersécurité au niveau matériel des systèmes informatiques, problématique commune à tous les domaines de l'informatique.

2 - À qui s'adresse ce dossier ?

Ce dossier s'adresse à la fois aux enseignants, aux techniciens et aux ingénieurs en ingénierie électrique ou en informatique embarquée.

Par sa grande complexité, abordée dans le paragraphe introductif, la cybersécurité est un domaine d'experts. Ce dossier n'a pas vocation à former des experts en cybersécurité. Il se propose au contraire de sensibiliser les acteurs travaillant dans des domaines concernés par la cybersécurité pour qu'ils puissent prendre en compte ces problématiques lors de la conception de systèmes.

En effet, la prise en compte des problématiques de cybersécurité dès la phase de conception d'un système avec l'application des bonnes pratiques et des solutions existantes est le plus souvent suffisante pour se protéger des attaques classiques réalisées par des individus malveillants isolés.

3 - Exemples d'attaques liées à des problématiques de cybersécurité

Cette partie présente trois exemples, issus des fiches d'incidents [1] publiées périodiquement par le Clusif, association française de promotion de la cybersécurité.

3.1 - Systèmes automatisés – Prise de contrôle du système de production d'une aciérie

Figure 2 : fiche 32 [1] : Prise de contrôle du système de production d'une aciérie

Cette fiche a été choisie car représentative des risques en cybersécurité des systèmes industriels et des conséquences importantes. L'intrusion a eu lieu par une campagne de mails frauduleux (*phishing*) et a permis de s'introduire sur le réseau de bureautique. De ce réseau bureautique, les hackers ont eu accès au réseau industriel pour prendre les commandes des systèmes de production et désactiver les mises en sécurité d'un haut fourneau jusqu'à provoquer de lourds dégâts.

La fiche rédigée par le Clusif à propos de cet incident propose les contre-mesures suivantes :

- Sensibilisation des agents aux méthodes d'attaque par *spear phishing* ;
- Restriction des droits accordés aux profils d'agent sur le réseau et les systèmes, de façon à détecter, voire empêcher toute action suspecte (prise de contrôle de systèmes, de terminaux…) ;
- Cloisonnement des réseaux de bureautique exposés aux attaques et aux intrusions, et des réseaux de contrôle des systèmes de production ;
- Mise en place de mécanismes de sûreté indépendants du système de conduite.

Parmi les fiches Clusif, un nombre important relate des attaques sur des systèmes industriels (exemple : empoisonnement de l'eau dans une usine de production d'eau, fiche 19) ou énergétiques (exemple : Black Energy, fiche 4 – coupure de l'électricité en Ukraine). La majeure partie pourrait être évitée par une bonne application des règles de cybersécurité abordées dans la partie 1 du dossier, consacrée aux systèmes automatisés industriels.

Quelques attaques sont le résultat d'un affrontement entre puissances étrangères, notamment l'attaque Stuxnet (fiche 36) qui a permis en 2010 aux services secrets israéliens de saboter les centrifugeuses iraniennes enrichissant l'uranium.

L'attaque Stuxnet en 2010 a révélé la vulnérabilité des systèmes automatisés et permis de prendre conscience des risques encourus et de la nécessité de mettre en œuvre une politique de cybersécurité pour les systèmes industriels également. Les nombreuses attaques qui ont suivi, comme celle présentée ici, mettent en évidence la lente formation des automaticiens à la cybersécurité et la longue marche vers la sécurisation de tous les équipements, pour certains en fonctionnement depuis longtemps.

3.2 - Objets connectés – Attaque sur une pompe à insuline

Quelques fiches s'intéressent aux objets connectés, notamment la fiche 41 qui présente la prise de contrôle à distance d'une pompe à insuline.

Figure 3 : Fiche 41 [1] : Attaque sur une pompe à insuline

Après l'analyse de la documentation constructeur (manuel d'utilisation, analyse des brevets, numéro de série de l'appareil…), un chercheur est parvenu à intercepter les communications échangées entre les capteurs et sa pompe à insuline et établir la liste des codes de commande utiles de l'équipement.

Le chercheur a alors imaginé plusieurs scénarios d'attaque : rejeu (l'entité malveillante intercepte puis réitère une transmission de données valide) de valeurs transmises à la pompe par les sondes, envoi de commandes forgées directement à la pompe (accès physique requis pour connaître le numéro de série nécessaire à l'envoi).

La fiche à propos de cet incident propose les contre-mesures suivantes :

- Forcer l'authentification mutuelle des sondes et pompes à insuline ;
- Chiffrer les signaux échangés ;
- En conclusion : intégrer la sécurité dans la phase de conception de ces objets.

Cette attaque met en valeur le manque de mesures de sécurité lors de la conception d'objets connectés. Les objets, parfois d'un coût peu élevé, sont conçus par des électroniciens qui valident le bon fonctionnement sans toujours connaître les attaques que leur dispositif risque d'affronter, parfois dans plusieurs années.

La fiche 22 du Clusif montre comment un adolescent a pu reproduire une télécommande d'aiguillage de Tramway. Martin Hron, chercheur en sécurité chez Avast, a publié pour sa part un article présentant la possibilité d'attaquer une machine à café connectée [3]. Les attaques peuvent porter uniquement sur la machine (dérèglement dangereux de la machine pouvant mener à sa destruction si une rançon n'est pas payée) mais aussi sur le réseau domestique (la machine à café sert de porte d'entrée au réseau).

La prise de contrôle d'objets connectés peu sécurisés (car peu chers et peu dangereux) permet à des hackers de lancer depuis ces milliers d'objets contrôlés des attaques DDoS (Distributed Denial of Service) en saturant un serveur de requêtes. Par exemple, le 21 octobre 2016, le malware Mirai, après avoir infecté des dizaines de millions d'objets connectés (notamment des caméras de surveillance de bébés, ce qui a participé à son succès médiatique) a rendu indisponible le gestionnaire de noms de domaine américain Dyn, ce qui a mis hors connexion les sites de clients importants comme Twitter, Spotify, et PayPal.

Une fois les objets connectés dans les mains de particuliers, non enregistrés et non visés par les attaques, il est très difficile de faire procéder à leur mise à jour, ce qui contribue à expliquer que Mirai refait parfois parler de lui.

La partie 2 du dossier, consacrée aux objets connectés, présente les dispositifs de cybersécurité sur les principaux réseaux IoT et une application pratique Bluetooth vulnérable et sa sécurisation.

3.3 - Systèmes embarqués – Prise de contrôle d'un véhicule automobile

En 2015, les chercheurs américains Chris Valasek et Charlie Miller ont révélé des failles de sécurité dans des applications embarquées dans un véhicule Jeep [2]. Ces failles concernaient un réseau Wifi disponible en option à l'intérieur du véhicule mais pouvaient aussi être exploitées directement par internet car les véhicules concernés étaient connectés au réseau cellulaire de l'entreprise Sprint.

Il fut alors possible de réaliser des commandes normalement gérées via le tableau de bord : augmentation du volume sonore de la radio, activation de la ventilation, etc. Ce sont de nombreuses commandes qui peuvent surprendre le conducteur et donc mener à des comportements dangereux sur la route.

Figure 4 : Fiche 23 [1] Prise de contrôle d'un véhicule automobile

La vulnérabilité la plus dangereuse était la possibilité de modifier le firmware du contrôleur V850 qui, a priori, ne pouvait que lire des informations sur le bus CAN mais ne pouvait pas y envoyer des commandes. Une fois le firmware modifié, les chercheurs ont réussi à envoyer des commandes à distance pour par exemple bloquer le système de freinage ou faire changer le véhicule de direction.

La fiche à propos de cet incident propose les contre-mesures suivantes :

- Utilisation d'un algorithme assurant une génération de clé non prédictible ;
- Mise en place d'un mécanisme empêchant la mise à jour du Firmware du contrôleur V850 par un code non signé ;
- Filtrage des communications entre le contrôleur V850 et le bus CAN

Cette attaque a fait l'effet d'un électrochoc dans l'industrie automobile en 2015 et a abouti au rappel de plus d'un million de véhicules. Ici, l'attaque est d'une complexité très élevée et a pris plusieurs années pour être conçue par les deux chercheurs. Elle souligne toutefois qu'avec l'augmentation de la connectivité, la cybersécurité est devenue un axe de travail important pour l'industrie automobile.

Deux autres fiches (exemples : 26, 27) montrent que les voitures modernes avec des logiciels de plus en plus complexes et des connectivités (wifi, 4G/5G, Bluetooth) importantes, notamment des interactions avec des applications smartphone, ont une surface vulnérable aux attaques plus importantes et deviennent des cibles de choix pour les hackers. Comme dans l'industrie, les mises à jour régulières et le cloisonnement du réseau multimédia et du réseau de terrain sont les premiers éléments mis en avant.

Enfin, la fiche 39 présente un exemple de leurre d'un récepteur GPS, menace prise très au sérieux, en particulier par les équipes travaillant sur les véhicules autonomes.

La partie 3 de ce dossier présente des vulnérabilités dans l'automobile et les travaux actuels des industriels pour renforcer la cybersécurité dans l'automobile.

4 - Plan du dossier

Après avoir défini la cybersécurité et le cadre de ce dossier, ces quelques exemples ont permis de souligner les problématiques de cybersécurité pour les systèmes industriels, dont une partie concernent des aspects réseaux : authentification, confidentialité, intégrité, non répudiation, disponibilité. C'est l'objet de la ressource « Fondamentaux de la sécurité réseau » [6], ce qui amène à introduire le plan prévu pour ce dossier :

Introduction à la cybersécurité des systèmes industriels

Fondamentaux de la sécurité réseau [6]

Cybersécurité des systèmes automatisés industriels

Cybersécurité des systèmes automatisés industriels [7]

Mise en œuvre du protocole sécurisé OPC-UA (à paraitre)

La Cybersécurité chez Eiffage Energie Systèmes [8]

Cybersécurité des objets connectés

Sécurité du protocole Bluetooth Low Energy (à paraitre)

Création d'une application Bluetooth Low Energy sur STM32WB (à paraitre)

Analyse de la sécurité d'une application Bluetooth Low Energy (à paraitre)

Sécurité du protocole LoraWan (à paraitre)

Sécurité du protocole Zigbee (à paraitre)

Wattsense - Siemens, une entreprise pour une GTB sécurisée [9]

Cybersécurité des systèmes embarqués (automobile)

(à paraitre)

Cybersécurité matérielle / les attaques par canaux auxiliaires

Mise en œuvre de la carte ChipWhisperer (à paraitre)

Références

[1]: *Fiches incidents cyber SI industriels – Fiche 22*, Clusif, 2022
https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/
[2]: *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, Andy Greenberg, WIRED, 2015
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[3]: *The Fresh Smell of ransomed coffee*, Martin Hron, Avast, 2020

https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/

[4]: Essonne : un centre hospitalier visé par une cyberattaque, une rançon de 10 millions de dollars exigée, Le Figaro, 2022

https://www.lefigaro.fr/secteur/high-tech/essonne-un-centre-hospitalier-vise-par-une-cyberattaque-une-rancon-de-10-millions-de-dollars-exigee-20220822

[5]: 10 choses à savoir sur les attaques DDoS massives contre Dyn, Le Monde informatique, 25 Octobre 2016, https://www.lemondeinformatique.fr/actualites/lire-10-choses-a-savoir-sur-les-attaques-ddos-massives-contre-dyn-66325.html

[6]: Fondamentaux de la sécurité réseau, M. Sechehaye, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/fondamentaux-dela-securite-reseau

[7]: Cybersécurité des systèmes automatisés industriels, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/cybersecurite-des-systemes-automatises-industriels

[8]: La Cybersécurité chez Eiffage Energie Systèmes, J. Zindy, F. Le Gall, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/cybersecurite-chez-eiffage-energie-systemes

[9]: Wattsense - Siemens, une entreprise pour une GTB sécurisée, M. Zenadi, M. Sauvergeat, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/wattsense-siemens-une-entreprise-pour-une-gbt-securisee

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay

Fondamentaux de la sécurité réseau

La Revue 3EI
Culture Sciences de l'Ingénieur

Édité le 16/02/2024

école normale supérieure paris-saclay

Maxime SECHEHAYE[1] - Anthony JUTON[2] - Magali SAUVERGEAT[3]

[1] *ENS Paris-Saclay – DER Nikola Tesla*
[2] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*
[3] *Enseignante BTS CIEL, Arpajon*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Si les attaques les plus nombreuses viennent de l'intérieur après une arrivée par mail (virus ou cheval de Troie téléchargé par un membre du personnel), nombre d'attaques parmi les plus spectaculaires exploitent les vulnérabilités des communications réseau. Avant d'aborder les différents champs d'application de la cybersécurité des systèmes industriels, cette ressource rappelle les principes fondamentaux de la sécurité réseau : confidentialité, intégrité, disponibilité, authentification et non-répudiation. Elle détaille ensuite le protocole TLS, très populaire, qui illustre trois de ces principes. La ressource se prolonge par une liste de vidéos d'illustration ou d'approfondissement, en français et en anglais, pouvant servir de support pour des séquences de classe inversée ou un co-enseignement anglais-GEII.

1 - Principes fondamentaux

Cette première partie présente les principes fondamentaux (confidentialité, intégrité, disponibilité, authentification et non-répudiation) de la cybersécurité qui, s'ils sont correctement implémentés, garantissent la protection via le réseau, excepté en cas d'exploitation de failles non documentées, ce qui est hors du champ de ce dossier.

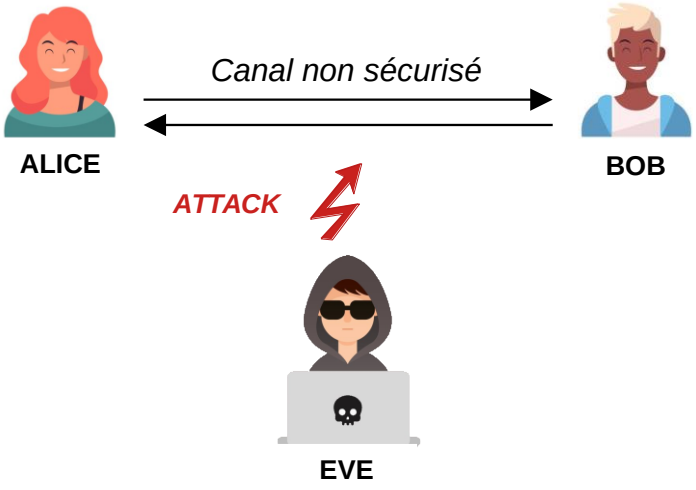


Figure 1 : Schéma simplifié d'une attaque

On imagine qu'Alice et Bob veulent échanger et que Eve souhaite nuire à leur relation. Alice et Bob peuvent être par exemple :

- Des personnes,
- Un terminal de paiement et un serveur de banque,
- Un automate industriel et sa supervision,
- Des calculateurs embarqués automobiles,
- Un smartphone et une serrure connectée.

Les communications sans fil peuvent être interceptées facilement et les communications sur Internet utilisent des chemins non connus et passent par des routeurs potentiellement écoutés. Le canal est donc souvent non sécurisé.

La **confidentialité** est l'impossibilité pour Eve de comprendre les messages circulant sur le canal, l'**intégrité** est la non-modification par Eve des messages (ou la détection d'une modification), l'**authentification** assure Bob que le message vient bien d'Alice et inversement, la **non répudiation** empêche Alice de nier avoir envoyé tel ou tel message et la **disponibilité** est la possibilité pour Bob et Alice de continuer à échanger.

1.1 - Confidentialité

La confidentialité permet de s'assurer que seules les personnes autorisées peuvent avoir accès à l'information transmise. Elle permet au concepteur d'un système d'information d'empêcher tout attaquant de récolter des informations sensibles en faisant de l'écoute clandestine (on parle d'*eavesdropping* en anglais).

La technique la plus courante pour garantir la confidentialité des échanges est l'utilisation de clés pour le **chiffrement** des données. Le chiffrement de données consiste en leur transformation en d'autres données, pas forcément de même longueur, grâce à un algorithme de chiffrement qui va utiliser une **clé** comme paramètre. Le terme clé est assez explicite : L'émetteur doit avoir une clé pour enfermer le message dans le coffre qui permet son transport et le destinataire doit aussi avoir une clé (la même ou une clé « associée ») pour ouvrir le coffre et lire le message.

Les algorithmes de chiffrement sont longs à développer et à vérifier. Les fuites survenant inévitablement, on ne peut envisager de redévelopper un algorithme de chiffrement à chaque fuite. C'est pourquoi le **Principe de Kerckhoffs** explique que l'algorithme doit être public et seules les clés doivent être secrètes. Celles-ci peuvent alors être renouvelées régulièrement.

On imagine ainsi qu'Alice souhaite envoyer un message à Bob. Ce message circulant sur un canal de communication accessible (ondes ou Internet par exemple), il peut être lu mais ne doit pas pouvoir être compris par Eve.

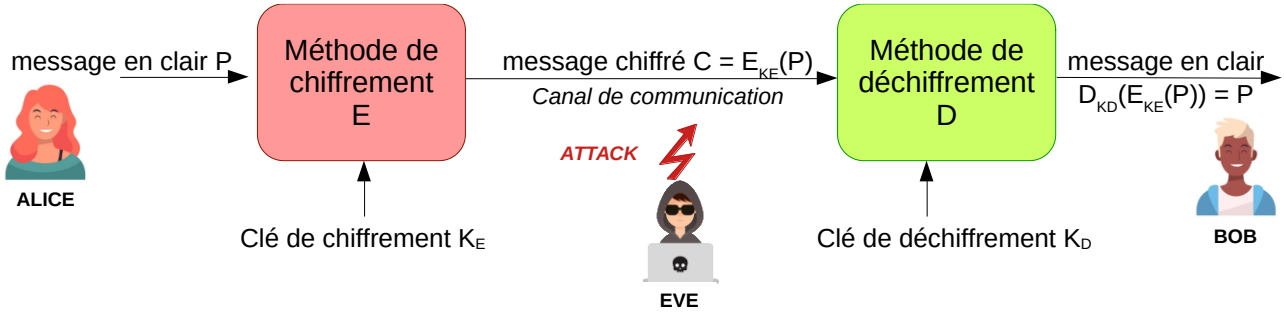


Figure 2 : Schéma de principe du chiffrement

Le développement des méthodes de chiffrement est la cryptographie, la recherche de méthode de déchiffrement sans connaître la clé est la cryptanalyse qui peut exploiter :

→ le texte chiffré seul,

→ un texte en clair connu (voir comme illustration le film *Imitation Game*),

→ un texte en clair choisi.

Chiffrement symétrique

Le chiffrement symétrique est le plus simple : l'émetteur et le récepteur **partagent le même secret**, la clé de chiffrement.

On peut imaginer par exemple deux individus qui discutent dans une langue qu'ils ont créée. La clé de chiffrement dans ce cas est le dictionnaire de cette langue. A priori, toute personne écoutant leur conversation et ne connaissant pas le dictionnaire de cette langue ne peut rien comprendre.

Un exemple classique de chiffrement symétrique est le **chiffrement par décalage** où l'on décale les lettres de l'alphabet d'un même nombre qui sera la clé de chiffrement. Par exemple, si l'on choisit un décalage de 5, `BONJOUR` sera chiffré en `GTSOTZW`. Pour déchiffrer le message, le récepteur doit seulement connaître la valeur du décalage et décaler les lettres dans le sens inverse. D'autres méthodes simples (OU exclusif avec un motif par exemple) consistent également à remplacer un caractère par un autre. On parle de **chiffrement par substitution**.

Il est aussi possible de modifier l'ordre des lettres, on parle alors de **chiffrement par permutation**.

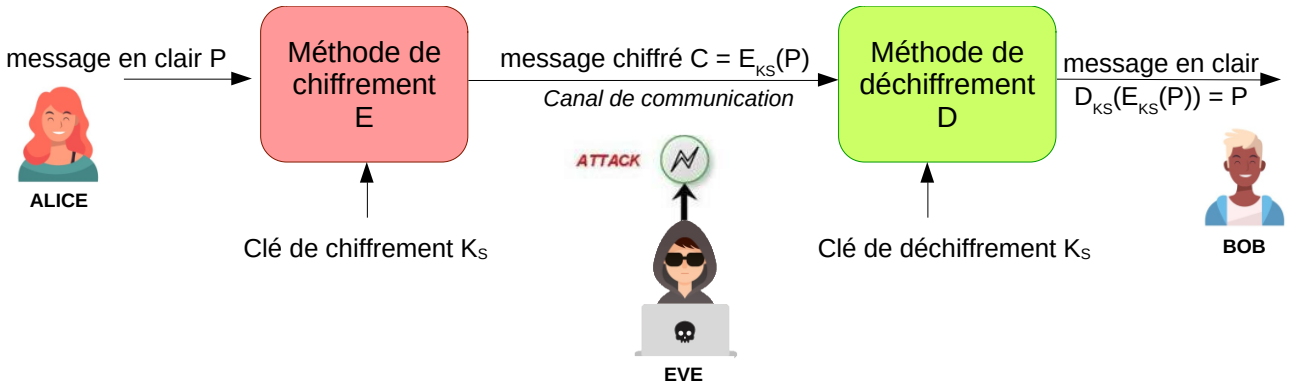


Figure 3 : Schéma de principe du chiffrement par clé symétrique

Un algorithme performant utilise à la fois permutation et substitution, pour éviter les méthodes de cryptanalyse statistique (pour du texte, on cherche le motif le plus courant et on lui associe la lettre la plus fréquente). Il utilise des clés suffisamment longues pour éviter les recherches de clés par force brute (tests successifs de toutes les clés possibles). L'algorithme de chiffrement symétrique le plus couramment utilisé (pour le wifi WPA2 ou pour HTTPS notamment) est l'algorithme **AES (Advanced Encryption Standard), avec des clés symétriques de 256 bits (soit 10^{77} clés possibles).**

> Les algorithmes de chiffrement symétriques sont plus rapides que les algorithmes de chiffrement asymétriques. Leur sécurité repose cependant sur le transfert de la clé secrète entre les deux appareils.

Chiffrement asymétrique

Le chiffrement asymétrique est plus complexe mais évite d'avoir à distribuer à l'avance une clé secrète aux participants : deux clés sont utilisées dans le processus de chiffrement : une **clé**

publique, connue de tous, et une **clé privée**, gardée secrète le plus souvent par le récepteur des données.

> La confidentialité des échanges est assurée lorsqu'on chiffre les données avec la clé publique : dans ce cas, seul le possesseur de la clé privée pourra déchiffrer le message.

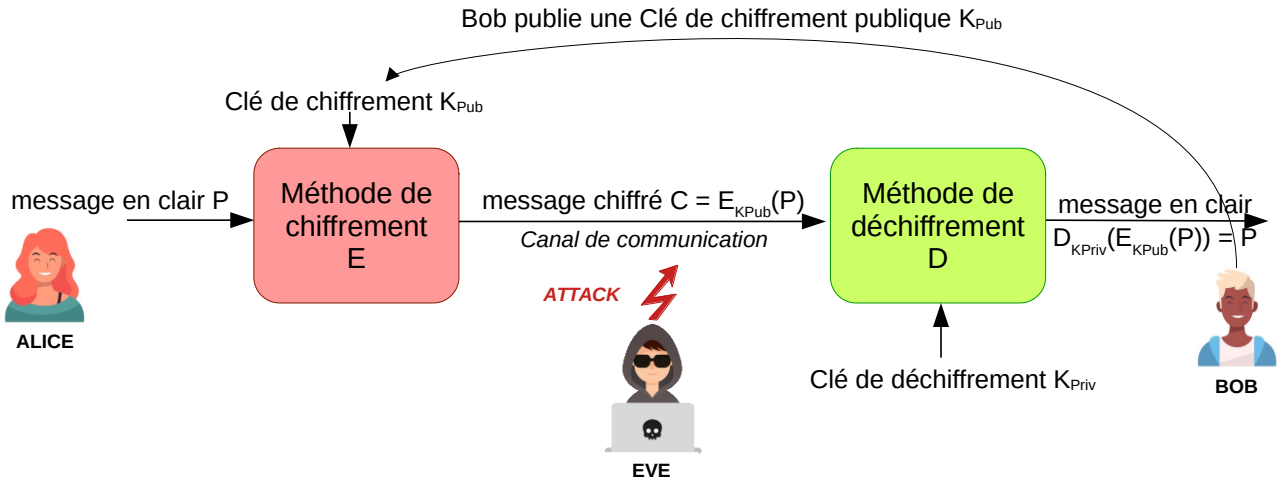


Figure 4 : Schéma de principe du chiffrement par clés asymétriques

Une analogie courante pour décrire le chiffrement asymétrique est celle de l'envoi d'un message de Bob vers Alice, en utilisant un coffre :

1° Alice dispose de cadenas identiques, s'ouvrant avec une clé et se refermant sans la clé (comme un cadenas classique). Elle envoie les cadenas ouverts à toute personne souhaitant lui envoyer un message secret, dont Bob. Elle garde la clé avec elle

2° Bob dispose d'un coffre et met son message à l'intérieur. Il prend le cadenas reçu d'Alice et le referme pour verrouiller le coffre.

3° Alice reçoie le coffre fermé avec son cadenas. Elle est la seule à pouvoir ouvrir ce cadenas.

L'algorithme de chiffrement asymétrique le plus souvent utilisé est l'algorithme **RSA**. Celui-ci est détaillé dans la ressource « Déchiffrez c'est gagné » [8], du même dossier.

Le protocole d'échange de clés **Diffie-Hellman** utilise aussi un algorithme asymétrique pour générer et partager de manière sécurisée une clé symétrique commune aux deux participants.

> Les algorithmes asymétriques sont les plus coûteux en ressources pour les calculs et en temps. Ils sont toutefois plus sécurisés que les algorithmes symétriques car aucune donnée secrète ne doit être partagée entre les deux protagonistes. On les utilise le plus souvent comme un moyen d'établir et de communiquer une clé symétrique à chaque nouvelle session (avec la méthode Diffie-Hellman par exemple).

On note que les clés publiques et privées de RSA sont réversibles, ce qui servira dans la partie suivante sur l'intégrité :

$D_{KPriv}(E_{KPub}(P)) = P$ mais aussi $D_{KPub}(E_{KPriv}(P)) = P$

1.2 - Intégrité

L'intégrité des données échangées désigne le fait qu'elles n'ont pas été modifiées durant le cycle de vie du message. Lors du téléchargement d'un logiciel par exemple, celui-ci n'est pas secret, il serait lourd de chiffrer l'ensemble du logiciel. Pour garantir l'intégrité du logiciel, l'éditeur met à disposition un code issu de l'ensemble des données de ce logiciel passé par une fonction de hachage cryptographique (**HMAC *Hash Message Authentication Code***).

Fonctions de hachage

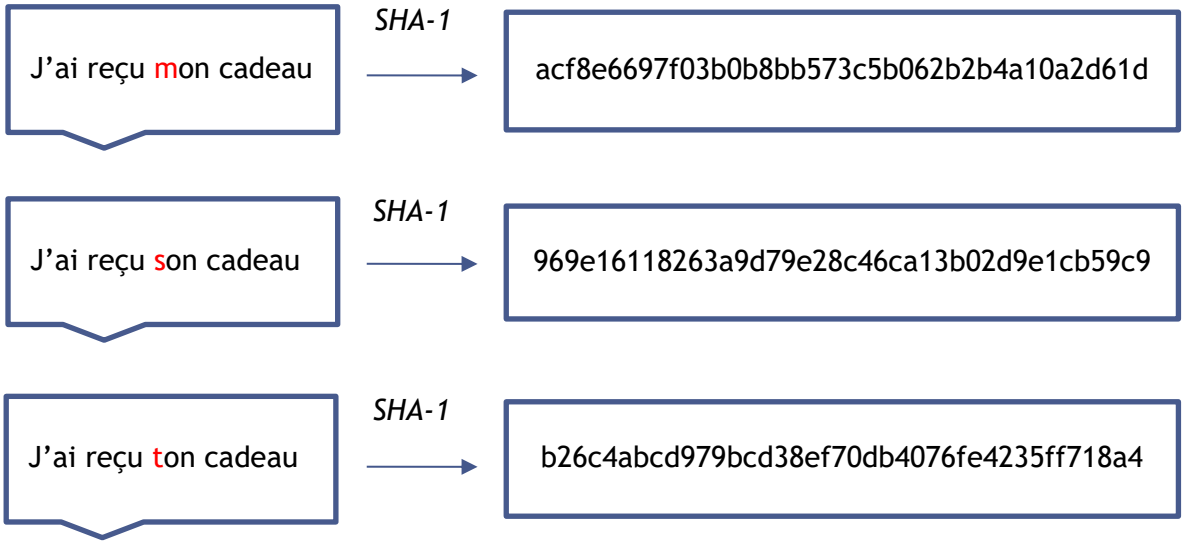
Les fonctions de hachage sont très souvent rencontrées en cybersécurité. Une fonction de hachage est une fonction qui, pour une donnée en entrée de longueur variable (qui peut être très longue, comme une vidéo ou un logiciel), retourne une valeur de longueur fixe (quelques octets), nommée condensat (ou en anglais *digest*).

Les codes de détection d'erreur CRC (Cyclic Redundancy Check) utilisés pour vérifier l'intégrité aux perturbations électromagnétiques des trames Ethernet ou CAN sont des fonctions de hachage, mais pas de cybersécurité.

Les fonctions de hachage classiques ne sont pas conçues pour répondre à toutes les problématiques de cybersécurité. C'est pourquoi on utilise des fonctions particulières, appelées **fonctions de hachages cryptographiques**. Les plus utilisées sont SHA-1 (*Secure Hash Algorithm*) et SHA-2, qui comprend notamment SHA-256.

Ces fonctions répondent aux exigences suivantes :

- Déterminisme : la même valeur de hachage (condensat) sera systématiquement générée pour un même message ;
- Rapidité de calcul ;
- **Non-réversibilité** : on ne peut pas reconstruire un message en ne connaissant que son condensat ;
- Résistance aux **collisions** : on ne peut pas trouver facilement un second message produisant le même condensat ;
- **Effet d'avalanche** : une légère modification du message entraîne une importante modification du condensat (voir exemple ci-dessous avec la fonction *SHA-1*).



Outre pour la signature numérique présentée ci-dessous, les fonctions de hachage sont utilisées pour le stockage des mots de passe. Les mots de passe ne sont normalement pas stockés en clair dans une application, pour éviter leur divulgation en cas de fuite. L'application se contente de stocker le condensat du mot de passe (mot de passe souvent concaténé avec une chaîne de caractère nommée « sel » pour améliorer la robustesse du stockage du condensat).

Signature numérique

On utilise ici la réversibilité des clés asymétriques. Si Alice chiffre un document avec sa clé privée K_{PRIVA}, qu'elle seule connaît, toute personne ayant la clé publique d'Alice peut déchiffrer le message et être sûr qu'il provient d'Alice.

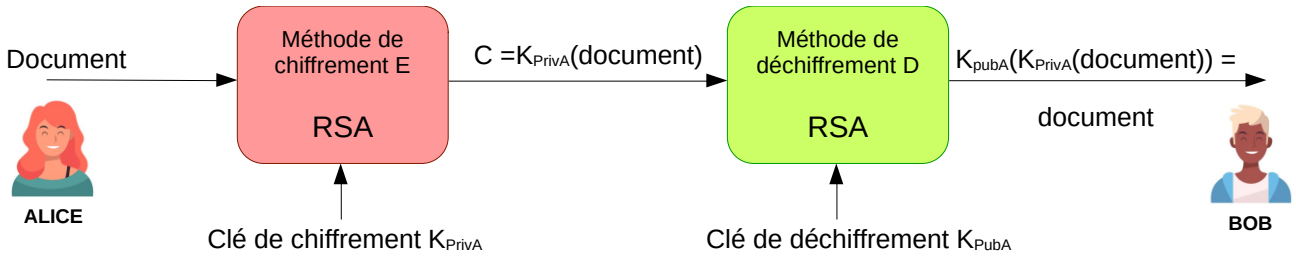


Figure 5 : Schéma de principe de la signature numérique

Cependant, chiffrer un gros fichier avec une clé asymétrique est gourmand en temps et en énergie. Il est plus économe de le hacher et de ne chiffrer avec la clé privée que le condensat.

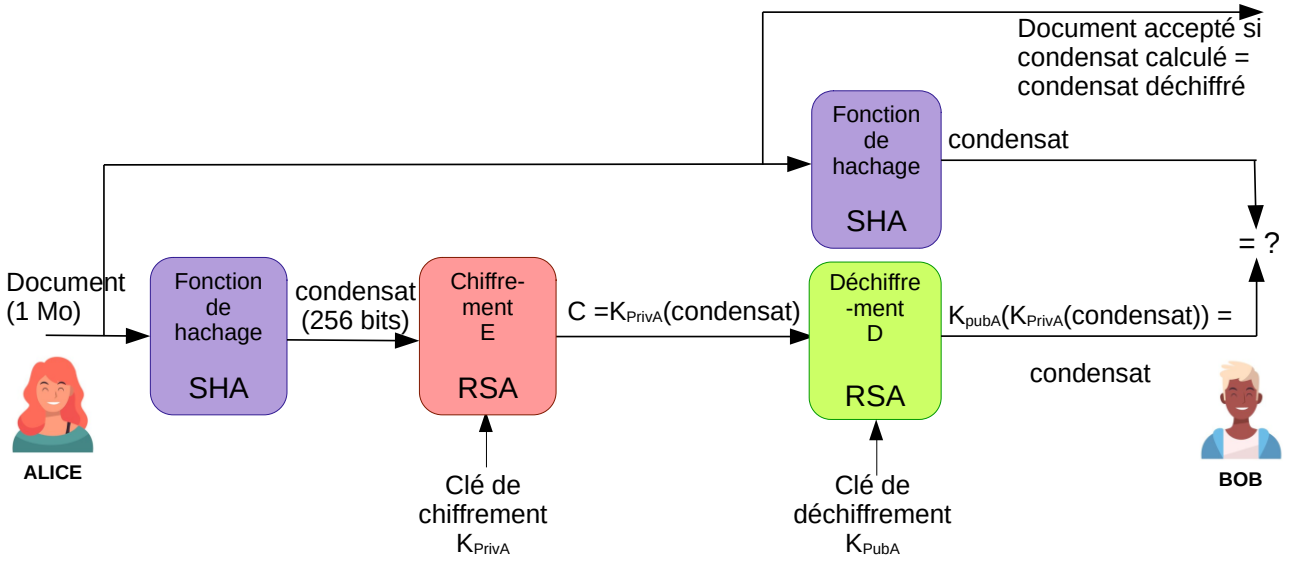


Figure 6 : Schéma de principe de la signature numérique avec fonction de hachage

Bob a ainsi l'assurance que le document reçu n'a pas été modifié entre son émission par Alice et sa réception.

1.3 - Non-répudiation

La non-répudiation assure qu'une action réalisée par une entité ne peut être niée ou ignorée. Elle apporte donc des preuves irréfutables qui pourront être utilisées a posteriori.

L'utilisation de **signatures numériques** peut assurer la non-répudiation. En chiffrant les messages avec sa clé privée (voir Figure 6), l'entité ne peut pas nier avoir signé le message car elle est la seule à posséder cette clé privée. De plus, certains mécanismes de signature numérique utilisent l'horodatage dans les données générant la signature numérique. Ainsi, même si la clé privée est volée par la suite, on peut s'assurer que la signature est bien valide car générée avant le vol.

1.4 - Authentification

L'authentification est le processus de vérification de l'identité d'une entité (utilisateur, système, appareil, etc.). Elle permet de s'assurer que, dans la communication, chacun est réellement qui il prétend être.

Les mécanismes d'authentification sont nombreux. On peut séparer d'une part les authentifications d'utilisateurs pré-enregistrés et les authentifications par **certificats**.

La première famille regroupe l'authentification par nom d'utilisateur et mot de passe ou l'authentification biométrique (empreinte digitale, reconnaissance faciale, etc.). Elle demande à l'un des partenaires de l'échange de connaître les identifiants de l'autre partenaire. Ce ne peut être une solution pour des échanges entre deux protagonistes ne se connaissant pas.

> Pour renforcer l'authentification, il est fréquent de mettre en place une authentification à plusieurs facteurs (deux voire trois). L'authentification à deux facteurs peut par exemple demander en plus d'un mot de passe la saisie d'une valeur envoyée par SMS.

Pour la seconde famille, on s'intéresse maintenant à deux acteurs ne se connaissant pas à l'avance, pour illustrer l'intérêt des certificats dans l'authentification.

La simple déclaration n'est évidemment pas suffisante, Eve pouvant déclarer être Alice.

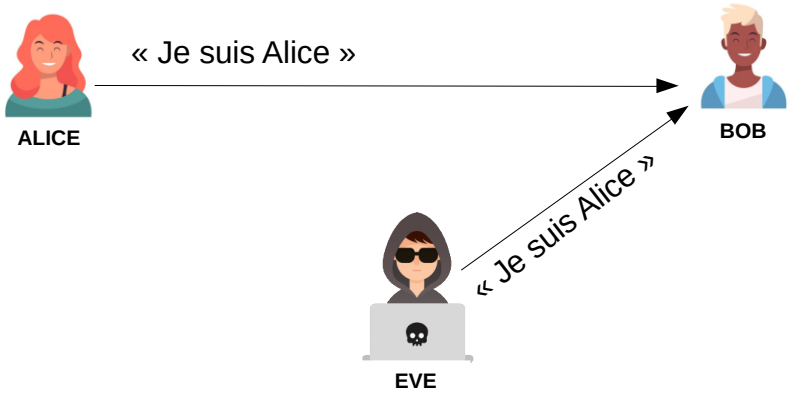


Figure 7 : Usurpation d'identité

Une déclaration chiffrée (ce qui demanderait d'avoir une clé symétrique) peut être rejouée par Eve pour se faire passer pour Alice.

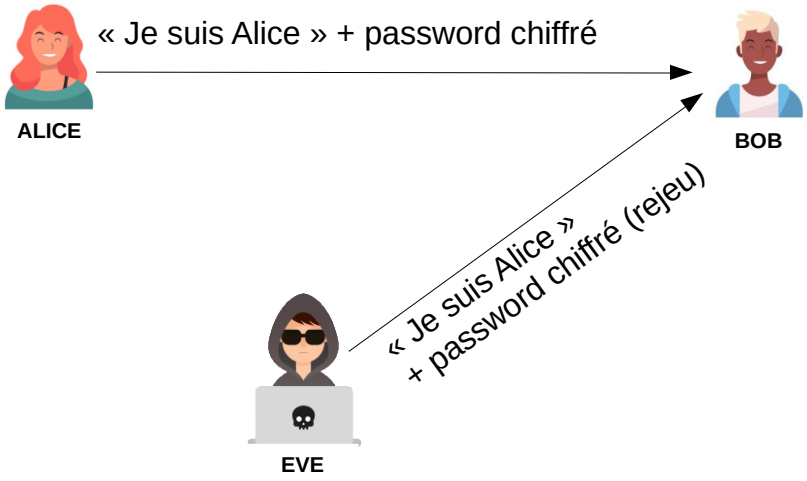


Figure 8 : Usurpation d'identité chiffrée par rejeu

Pour éviter le rejeu, Bob envoie un nombre R à usage unique. Comme les acteurs n'ont pas partagé au préalable une clé secrète, un mécanisme à clés asymétriques est utilisé. K_{PUBA} et K_{PRIVA} sont les clés publiques et privées d'Alice. Alice renvoie R chiffré avec sa clé privée et diffuse sa clé publique. On joue sur la réversibilité des clés publiques et privées. En connaissant la clé publique d'Alice, Bob (et toute autre personne voyant passer le message) peut déchiffrer le message $K_{PrivA}(R)$ et donc être sûr qu'il provient d'Alice.

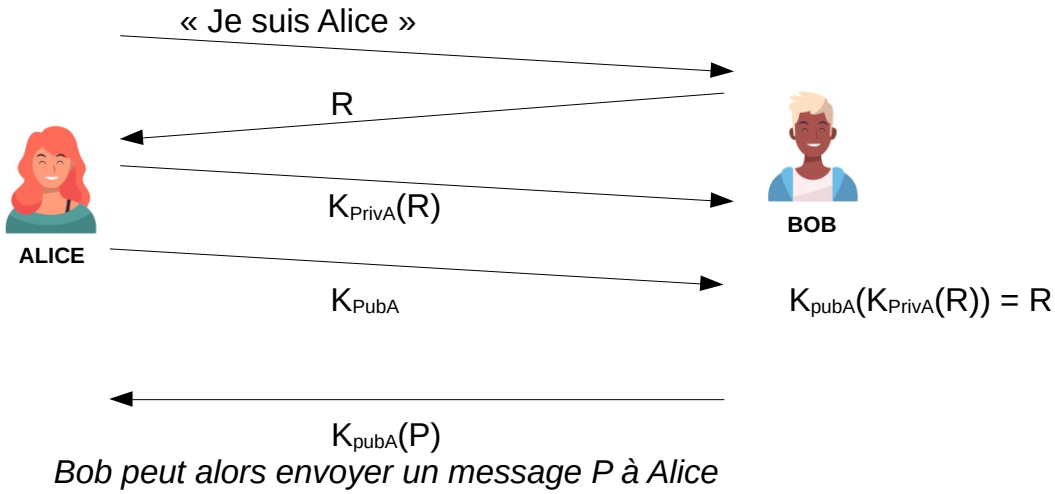


Figure 9 : Authentification par signature d'un nombre R

Reste à être sûr que K_{pubA} est bien la clé publique d'Alice. En effet, il est possible d'imaginer qu'Eve s'interpose entre Bob et Alice et intercepte les communications de l'un comme de l'autre. On appelle cette attaque « Man in the Middle ». Eve se fait passer pour Alice auprès de Bob et pour Bob auprès d'Alice. Elle peut alors lire et/ou modifier le message P envoyé par Bob à Alice.

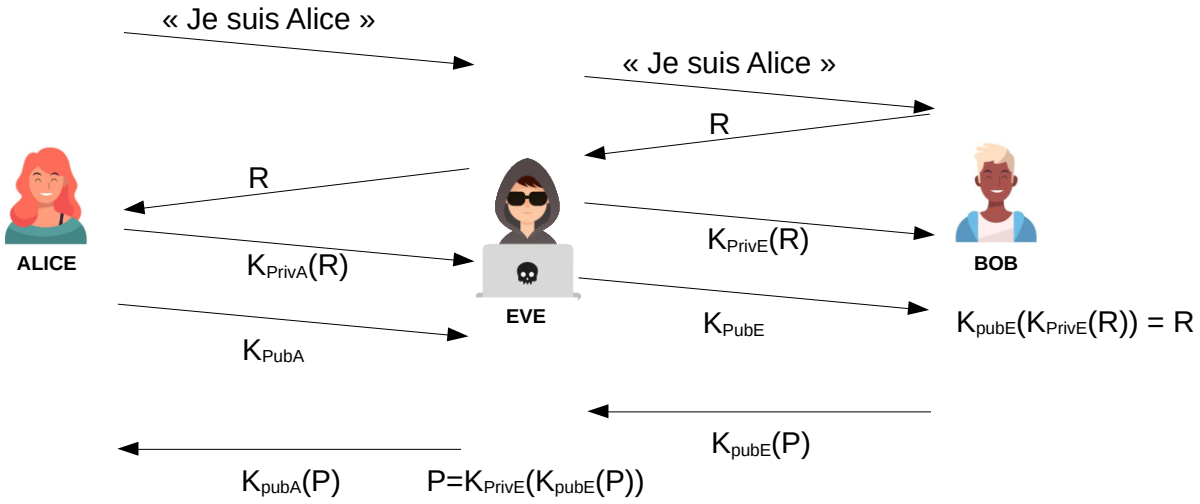


Figure 10 : Principe de l'attaque Woman in the middle

Il est donc nécessaire de certifier les clés publiques, ce que permettent les certificats. X509 est le protocole de gestion de certificats le plus populaire. Un tiers de confiance nommé autorité de certification signe numériquement (c'est-à-dire chiffre avec sa clé privée un condensat) le certificat contenant notamment la clé publique et le nom du protagoniste. La clé publique de cette autorité de certification est connue (les navigateurs web ont par exemple les clés publiques des principales autorités de certification) ou alors elle est diffusée elle-même avec un certificat d'une autorité de certification connue.

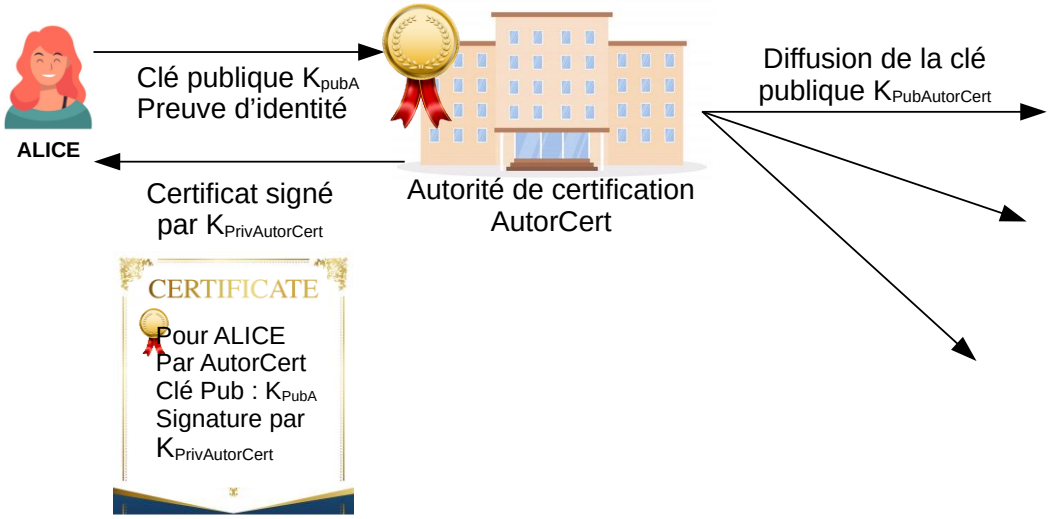


Figure 11 : Obtention d'un certificat auprès d'une autorité de certification

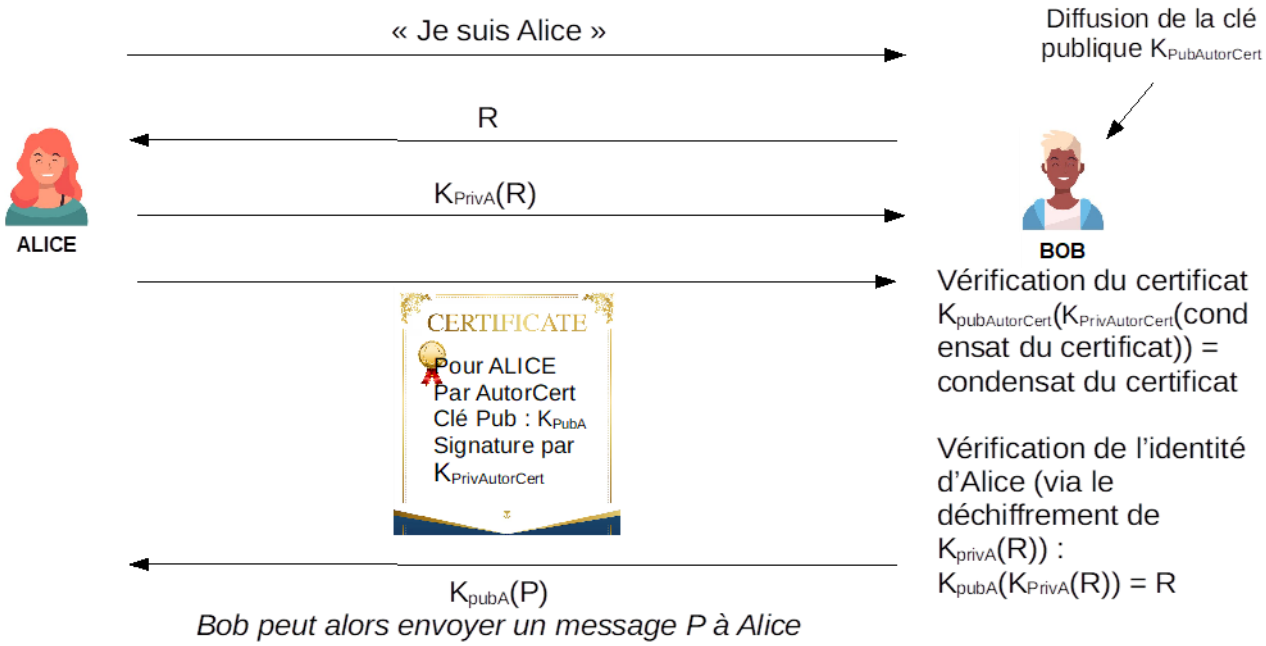


Figure 12 : Authentification avec utilisation d'un certificat

On résout ainsi le risque d'usurpation d'identité par Eve. On retrouve ces concepts en vidéo sur la chaîne d'Hervé Discours [7].

Figure 13 : Copie d'écran de la vidéo d'Hervé Discours sur les clés et certificats

1.5 - Disponibilité

La disponibilité désigne la capacité d'un service, d'un système à être accessible par un utilisateur autorisé quand il le souhaite.

> La disponibilité d'un système d'information est l'un des piliers de son bon fonctionnement. En effet, une attaque rendant impossible l'accès à un service en ligne fourni par une société nuit grandement à l'image de cette dernière.

Les attaques par déni de service distribué (DDoS, Distributed Denial of Service) sont particulièrement difficiles à bloquer car elles n'utilisent que des requêtes légales, issues d'appareils détournés, pour saturer un serveur. Les dernières attaques DDoS atteignent des débits de plusieurs $Tb.s^{-1}$ (2,3 $Tb.s^{-1}$ pour l'attaque d'AWS en février 2020)

Les requêtes étant légales, les mécanismes permettant de garantir la disponibilité sont complexes mais très étudiées au vu des enjeux financiers ou organisationnels liés à la coupure de service réseau :

- **Redondance** des systèmes ;
- Répartition de la charge de travail sur plusieurs serveurs pour éviter la surcharge ;
- Filtrage en amont des requêtes avec des pare-feux avancés.

2 - Exemple du protocole TLS

Le protocole TLS (*Transport Layer Security*, sécurité de la couche de transport) est un protocole cryptographique permettant de sécuriser les communications sur un réseau informatique (ici confidentialité via une clé symétrique AES-128, intégrité via une fonction de hachage SHA-256 et authentification via un certificat X509 et des échanges par clés asymétriques Diffie Hellman), au-dessus de la couche transport TCP et en-dessous de la couche application. Son utilisation la plus connue est le protocole HTTPS qui consiste en une version sécurisée du protocole HTTP. Il est aussi utilisé pour des protocoles industriels (OPC UA, IEC61850) et dans l'automobile (IEC15118).

> On utilise parfois le terme « SSL/TLS ». SSL désigne l'ancêtre du protocole TLS et toutes ses versions sont obsolètes depuis 2015. Il convient donc d'utiliser uniquement le terme TLS dans la conception d'un système d'information et de ne pas utiliser abusivement le terme « SSL/TLS ».

Cette partie explique les principes de fonctionnement de ce protocole afin d'illustrer l'implémentation des principes fondamentaux exposés précédemment. La version 1.3 étant un peu plus simple que la 1.2, elle sert de support à cette explication. Les principes sont les mêmes, avec un peu plus d'échanges pour la version 1.2, encore utilisée.

2.1 - Négociation de la connexion sécurisée

Dans un premier temps, le client demande au serveur de s'authentifier, les deux se mettent d'accord sur les paramètres de la connexion sécurisée et, via des clés asymétriques, échangent les clés symétriques de session.

Premier contact par le client - *Client Hello*

Dans ce premier message, le client communique entre autres au serveur les versions de TLS qu'il prend en charge, l'ensemble des algorithmes cryptographiques qu'il peut utiliser par ordre de préférence et un nombre aléatoire qui servira pour générer les clés de cette session. Pour reprendre une session interrompue, il est possible de fournir un identifiant de session, *Session ID*.

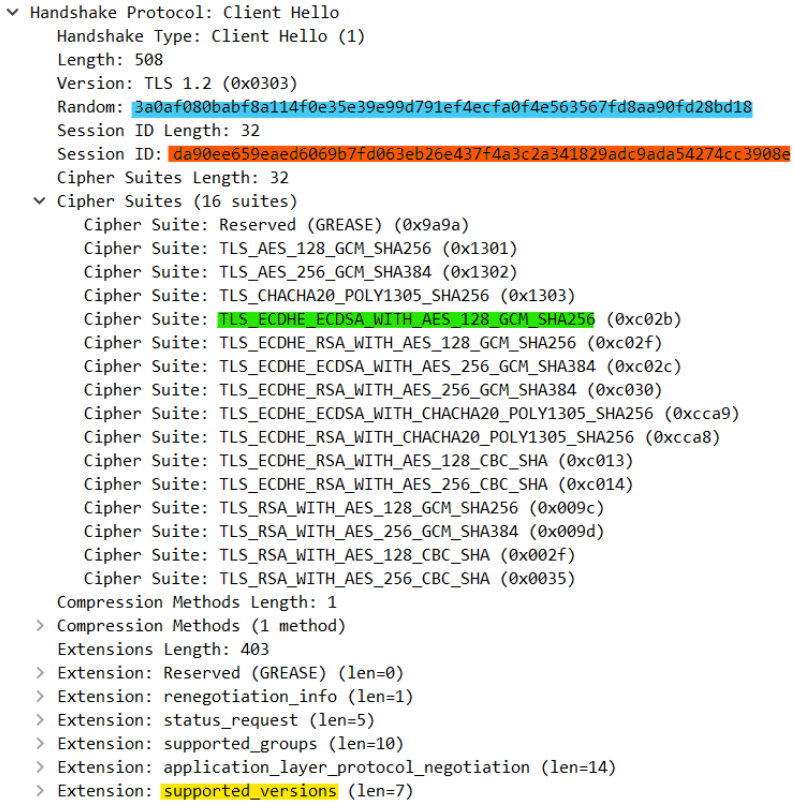


Figure 14 : Extrait d'un ClientHello sur Wireshark

Il est intéressant d'analyser les types d'algorithmes cryptographiques utilisés :

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Elliptic Curve Diffie-Hellman Ephemeral

Algorithme asymétrique qui permet la génération et l'échange d'une clé symétrique utilisée pour l'établissement des clés de session

Elliptic Curve Digital Signature Algorithm

Algorithme asymétrique qui permet l'authentification, la non-répudiation et l'intégrité.

AES 128 bits Galois/Counter Mode

Algorithme de chiffrement symétrique qui permet la confidentialité des communications

Secure Hash Algorithm 256 bits

Fonction de hachage qui permet de générer un condensat pour vérifier l'intégrité des données échangées

Réponse du serveur - *Server Hello*

Le serveur répond alors au client en sélectionnant pour chaque paramètre une valeur parmi celles proposées par le client et qui convient à ses capacités.

Le serveur envoie également un nombre aléatoire qui servira pour générer les clés de cette session

Envoi et vérification du certificat du serveur

Le serveur fournit ensuite au client un certificat électronique, aussi appelé certificat numérique. Il va permettre au client de faire confiance à l'entité avec laquelle il communique. Il s'agit donc d'une étape essentielle pour garantir la sécurité de la connexion qui est sur le point d'être établie.

On peut considérer ce certificat comme la carte d'identité du serveur. On observe sur la Figure 15 le certificat numérique du site de l'ENS Paris-Saclay (accessible en cliquant sur le cadenas dans la barre d'adresse).

Figure 15 : lecture du certificat numérique du site de l'ENS Paris-Saclay sur un navigateur Google Chrome

Le certificat numérique est émis par une autorité de certification. Sur la Figure 15, le certificat a été fourni par l'organisation GEANT. Cette organisation fournit, moyennant rétribution, le certificat pour une période donnée, cette période est d'un an pour celui de la Figure 15.

> Il existe de nombreuses autorités de certifications qui opèrent à différentes échelles. Cela permet de ne compromettre que les serveurs situés dans une zone précise si une autorité de certification n'est plus sûre. Ainsi, les autorités de certification intermédiaires doivent aussi présenter un certificat numérique et le client doit vérifier tous les certificats numériques jusqu'à remonter à une autorité de certification de confiance.

Le client va donc devoir :

- Vérifier l'intégrité du message avec le condensat (condensant nommé « Empreinte SHA » sur la Figure 15) ;
- Vérifier l'authentification grâce à la signature du certificat par la clé privée de l'autorité de certification ;
- S'assurer qu'il peut faire confiance à l'autorité de certification en remontant la chaîne des certificats numériques, c'est-à-dire en vérifiant les certificats des autorités de certification jusqu'à arriver sur une autorité de certification de référence, connue du logiciel (le navigateur pour HTTPS par exemple) (voir Figure 16).

Figure 16 : Chaîne de vérification des certificats pour le site de l'ENS Paris-Saclay

Calcul du secret partagé

L'algorithme de Diffie Hellman, un peu différent de RSA, permet d'établir une clé commune à partir d'éléments de clés publiques envoyés par les 2 acteurs. Chacun peut alors déchiffrer à l'aide de sa clé privé les échanges.

Le client connaît désormais via le certificat les éléments de clés publiques du serveur et a transmis les siens lors du premier échange. Indépendamment, le client et le serveur vont donc pouvoir calculer à partir de ces éléments de clés publiques un nouveau secret commun, le *master secret*.

Calcul des clés de session

Le client peut alors communiquer de manière chiffrée avec le serveur, par le *master secret*. Il peut ainsi envoyer des clés symétriques AES au serveur, de manière chiffrée. 4 clés sont partagées : 1 pour les données client → serveur, 1 pour la vérification de l'intégrité client → serveur et la même chose dans le sens serveur → client.

Les différentes données utilisées pour établir la sécurité de l'application (valeurs aléatoires, *pre-master secret*, *master secret*, etc.) ne seront pas réutilisées lors de futures sessions entre les mêmes client et serveur. Cela participe au respect d'un principe appelé « confidentialité persistante » (*Forward Secrecy* en anglais) qui garantit que la découverte d'un secret privé ne compromet pas la confidentialité des échanges passées.

2.2 - Établissement de la connexion sécurisée

Une fois les clés de session établies, le client et le serveur vont chacun envoyer un message permettant de vérifier qu'ils possèdent bien les mêmes clés et signalant que les échanges futurs seront chiffrés.

Les échanges sont à présent sécurisés.

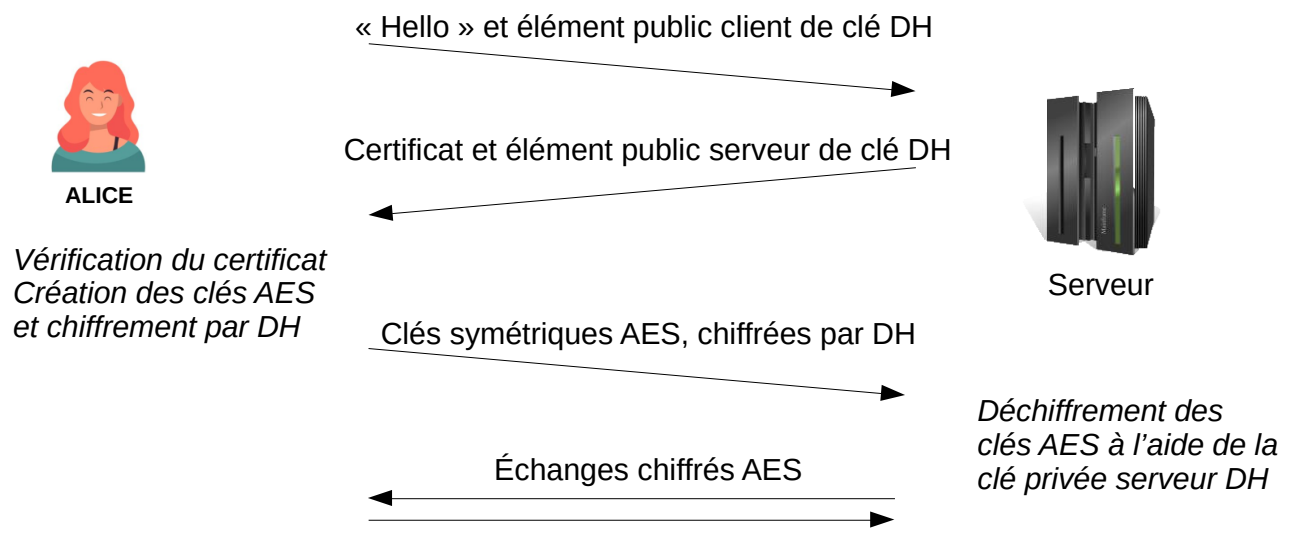


Figure 17 : Echanges TLS 1.3 menant à la mise en place d'une communication sécurisée

Les acquisitions ci-dessous présentent une acquisition wireshark de la mise en place d'un échange TLS 1.2 et TLS 1.3. Seuls les messages TLS sont affichés, les acquittements TCP notamment n'apparaissent pas, pour plus de lisibilité. Application Data signifie que les échanges chiffrés sont commencés.

Source	Destination	Protocol	Length	Info
192.168.1.41	129.175.212.146	TLSv1.2	744	Client Hello
129.175.212.146	192.168.1.41	TLSv1.2	1434	Server Hello
129.175.212.146	192.168.1.41	TLSv1.2	1430	Certificate
129.175.212.146	192.168.1.41	TLSv1.2	354	Server Key Exchange, Server Hello Done
192.168.1.41	129.175.212.146	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
129.175.212.146	192.168.1.41	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
192.168.1.41	129.175.212.146	TLSv1.2	1930	Application Data
129.175.212.146	192.168.1.41	TLSv1.2	685	Application Data

192.168.1.41	138.231.176.51	TLSv1.3	721	Client Hello
138.231.176.51	192.168.1.41	TLSv1.3	4150	Server Hello, Change Cipher Spec, Application Data
138.231.176.51	192.168.1.41	TLSv1.3	2739	Application Data, Application Data, Application Data
192.168.1.41	138.231.176.51	TLSv1.3	134	Change Cipher Spec, Application Data
192.168.1.41	138.231.176.51	TLSv1.3	679	Application Data
138.231.176.51	192.168.1.41	TLSv1.3	325	Application Data

Figure 18: Comparaison entre l'établissement d'une connexion TLS 1.2 et celui d'une connexion TLS 1.3

3 - Conclusion

Cette ressource a expliqué les principes fondamentaux de la sécurité réseau que l'on retrouvera dans les autres ressources de ce dossier avant de voir comment ces principes sont mis en œuvre par le protocole TLS.

La ressource associée « Informatique débranchée : Déchiffrez c'est gagné » [8] donne un exemple de mise en pratique des algorithmes de chiffrement par les étudiants.

Les principes présentés ici sont issus de l'informatique et appliqués en automatisme industriel (OPC UA, IEC 61850, …) ou dans l'automobile (IEC 15118). Dans les objets connectés, aux capacités de calcul et à la consommation plus réduites, il est important d'appliquer les mêmes principes, avec des algorithmes peu gourmands. Cela passe notamment par l'intégration hardware de blocs de chiffrement, ce qui fige les algorithmes utilisés.

Par ailleurs, la puissance des ordinateurs augmentant, la taille des clés croît également pour résister aux attaques par force brute, passant par exemple de 1024 à 2048 bits pour RSA. Cela pose la question de la mise à jour logicielle, voire matérielle, des systèmes industriels à la longue durée de vie.

Enfin, l'arrivée des premiers ordinateurs quantiques, avec des capacités estimées très importantes pour craquer les clés asymétriques, amène dès aujourd'hui à réfléchir à de nouveaux algorithmes de chiffrement, plus robustes face à ces nouvelles machines. Que restera-t-il alors de la sécurité réseau des systèmes industriels installés en 2024 ?...

4 - Annexe : Quelques références supplémentaires

Cette annexe propose une sélection de vidéos YouTube, en français ou en anglais, permettant d'illustrer ou d'approfondir les différentes notions expliquées dans cette ressource.

Cette sélection restreinte parmi les nombreuses vidéos sur le sujet permet aussi de découvrir quelques chaînes YouTube dédiées à la sécurité réseau. Le lecteur intéressé par la pédagogie ou le niveau technique d'une des vidéos pourra explorer les autres vidéos de la chaîne.

Ces vidéos peuvent être utilisées notamment pour réaliser des séquences pédagogiques sous forme de classe inversée ou comme supports pour le co-enseignement en anglais en BTS CIEL.

4.1 - Exemples d'attaques liées à des problématiques de cybersécurité

La chaine **Cyber Vox** regroupe des vidéos, en français et en anglais, sur des attaques historiques telles que Wannacry, notPetya, stuxnet solarWinds : https://www.youtube.com/@CyberVox

4.2 - Principes fondamentaux : Vidéos de vulgarisation

4.2.1 - Confidentialité

Chiffrement symétrique / Chiffrement asymétrique

Cette vidéo de vulgarisation sur le chiffrement symétrique et asymétrique, issue de la chaîne en anglais Code.org, s'appuie sur des animations très pédagogiques :

The Internet : Encryption & Public Keys : https://www.youtube.com/watch?v=ZghMPWGXexs

La chaine Exo7Math apporte les notions mathématiques pour comprendre le protocole RSA du point de vue algorithmique :

Cryptographie - partie 5 : arithmétique pour RSA : https://youtu.be/M7vOxKVLsVY

Cryptographie - partie 6 : chiffrement RSA : https://www.youtube.com/watch?v=Xlal_d4zyfo

4.2.2 - Intégrité

Fonctions de hachage

Cette vidéo, issue de la chaîne **Bande de Codeurs**, détaille les fonctions de hachage et leurs différentes utilisations :

Comprendre les fonctions de HACHAGE : https://www.youtube.com/watch?v=OHXfKCH0b6s

4.2.3. - Disponibilité

Cette vidéo issue de la chaîne **@IBM technology** aborde la résistance aux ransomware :

Protecting Yourself from Ransomware : https://www.youtube.com/watch?v=eizn9TC68E8

4.2.4 - Authentification

Cette vidéo de la chaîne **kubucation,** en anglais, approfondit les notions de certificat et d'autorité de certification appliquées à HTTPS :

How does HTTPS work? What's a CA? What's a self-signed Certificate? :
https://www.youtube.com/watch?v=T4Df5_cojAs

4.2.5 - Non-répudiation

La chaîne **LeDroitpourMoi** propose une vidéo s'intéressant au côté juridique de la signature électronique :

Signature électronique : comment ça marche ? https://www.youtube.com/watch?v=GhTZUbp9M-8

4.3 - Sujets divers

La chaîne L'informateur aborde en français tous les sujets de la sécurité réseau, notamment les réseaux VPN.

Sécurité 13 : IPSec et comment fonctionne un VPN :
https://www.youtube.com/watch?v=V9bTy0gbXIQ&list=PLOapGKeH_KhFBC39ltMDhkEx1aI3hlwSK

La chaîne **@IBM technology** présente, en anglais, le concept Zero Trust :
Why Implement Zero Trust : https://www.youtube.com/watch?v=lT11tGaEC3s

Références

[1]: *Fiches incidents cyber SI industriels – Fiche 22*, Clusif, 2022
https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/

[2]: *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, Andy Greenberg, WIRED, 2015
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3]: *The Fresh Smell of ransomed coffee*, Martin Hron, Avast, 2020
https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/

[4]: *Essonne : un centre hospitalier visé par une cyberattaque, une rançon de 10 millions de dollars exigée*, Le Figaro, 2022
https://www.lefigaro.fr/secteur/high-tech/essonne-un-centre-hospitalier-vise-par-une-cyberattaque-une-rancon-de-10-millions-de-dollars-exigee-20220822

[5]: Images issues de Freepik : https://fr.freepik.com/vecteurs-libre/avatars-gens-heureux_7085154.htm et https://fr.freepik.com/vecteurs-libre/jeune-pirate-anonyme-au-design-plat_2753360.htm et https://fr.freepik.com/vecteurs-libre/ensemble-batiments-ville_8270967.htm

[6]: Computer Networks, Andrew Tanenbaum, Nick Feamster, David Wetherall, Pearson Education Limited

[7]: Cybersécurité, Clés publique/privée, Certificat X509, PKI, Chiffrement RSA, fichier.pem OPC-UA, Hervé Discours, https://www.youtube.com/watch?v=58FUQzWxs3Y

[8]: Informatique débranchée : Déchiffrez c'est gagné, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/informatique-debranchee-dechiffrez-cest-gagne

[9]: Computer Networking, a top-down approach, Jim Kurose, Keith Ross, Pearson; 8th edition (September 13, 2020), http://gaia.cs.umass.edu/kurose_ross

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay

Informatique débranchée : Déchiffrez c'est gagné

La Revue 3EI
Culture Sciences de l'Ingénieur
école normale supérieure paris-saclay

Anthony JUTON[1]

Édité le 13/02/2024

[1] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

La ressource « Fondamentaux de la sécurité réseau » [2] présente notamment les principes de chiffrement symétrique et asymétrique. Pour illustrer le cours, parfois un peu théorique, est née cette activité ludique d'informatique débranchée. L'objectif de l'activité est de sensibiliser les étudiants aux mécanismes de communication sur canal non sécurisés en pratiquant un peu de chiffrement par clés symétriques et asymétriques, dans l'esprit du protocole TLS.

L'activité est présentée comme elle a eu lieu en décembre 2023, avec 20 étudiants de Master, pendant le cours de réseau. Des adaptations ou une assistance de l'enseignant sont à prévoir en fonction du niveau en mathématiques des étudiants. Une version 2 est en réflexion pour faire intervenir l'authentification par certificat.

1 - Le contexte et les règles du jeu

Trois équipes de 6/7 étudiants séparées en 2 chiffreurs, 2 déchiffreurs et 2 hackeurs (répartition variable suivant les équipes).

Les chiffreurs doivent faire deviner un mot de 8 lettres reçu dans une enveloppe aux déchiffreurs. Le seul moyen de communication, non sécurisé, est un tableau commun pour tous. Tout le monde joue en même temps. Les calculatrices sont autorisées.

Le premier mot déchiffré vaut 3 points, le deuxième vaut 2 points et le dernier vaut 1 point, qu'il soit déchiffré par l'équipe associée à ce mot ou par le hackeur d'une autre équipe (l'équipe du hackeur obtient alors le ou les points).

Le protocole proposé est inspiré de TLS (le déroulement précis est décrit en partie 4) :

1. Le chiffreur calcule et diffuse une clé publique RSA via le tableau.
2. Le déchiffreur reçoit la clé publique et l'utilise pour chiffrer une clé symétrique créée pour l'occasion (type AES, mais plus simple) et l'envoyer via le tableau.
3. Le chiffreur utilise alors la clé symétrique pour chiffrer le mot à faire deviner et envoie le mot chiffré à ses partenaires via le tableau.
4. Le déchiffreur déchiffre le mot et annonce la réponse.

Pendant ce temps, les hackeurs tentent de craquer les clés privées adverses pour obtenir la clé symétrique, déchiffrer le mot de l'équipe adverse avant elle et obtenir le point.

2 - Le protocole à clé symétrique

TLS utilise le protocole à clé symétrique AES-128 ou AES-256. AES combine des substitutions et des permutations. Pour faire simple et rapide à chiffrer, on utilise uniquement des substitutions, avec un Ou exclusif utilisant une clé symétrique 20 bits.

Les caractères, uniquement des lettres majuscules, sont codés sur 5 bits.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Exemple : coder GEII avec la clé 0xabcde puis déchiffrer le message chiffré avec la même clé.

```
Message GEII      : 00111001010100101001
XOR clé 0xabcde   : 10101011110011011110
Message chiffré   : 10010010100111110111


Message chiffré   : 10010010100111110111
XOR clé 0xabcde   : 10101011110011011110
Message déchiffré : 00111001010100101001
                      G    E    I    I
```

Pour le jeu, on utilise une clé de 20 bits et un algorithme de chiffrement Ou exclusif. Le mot à chiffrer faisant 8 caractères, on concatène la clé avec elle-même pour chiffrer 40 bits.

3 - Le protocole à clés asymétriques RSA

Pour transmettre les clés symétriques, on utilise l'algorithme de chiffrement à clé publique RSA, également utilisé par TLS 1.2 (mais plus par TLS 1.3).

Algorithme à clé publique RSA (du nom de ses inventeurs Rivest, Shamir, Adleman)

- Choisir deux grands nombres premiers p et q (p et q sont normalement des nombres sur 1024 voire 2048 bits).
- Calculer n = p * q et z = (p-1)*(q-1)
- Choisir un nombre d (d<n) tel que d et z n'aient pas de facteur commun
- Trouver e tel que e * d = 1 mod z
- Former des blocs de k bits tels que 2^k<n

- Calculer pour chaque bloc $C=P^e \bmod n$
- Déchiffrer en calculant $P = C^d \bmod n$

{e,n} est la clé publique

{d,n} est la clé privée

C'est réversible : le contraire ({d,n} publique et {e,n} privée) marche aussi

Exemple, p = 3, q = 11, d=7. Chiffrer « ENS ».

Les caractères, uniquement des lettres majuscules, sont codés sur 5 bits.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

On trouve n = 33, z = 20

On choisit d = 7 (7<33 et 7 et 20 n'ont pas de facteur commun)

On trouve e = 3 (3*7 = 21 = 1 mod 20)

On choisit k = 5 ($2^5 = 32 < 33$)

Chaque caractère est un bloc. P = {E,N,S} = {5,14,19}.

On le chiffre avec la clé publique {e,n} = {3,33}

- E → $55^3 \bmod 33 = 26$
- N → $1414^3 \bmod 33 = 5$
- S → $1919^3 \bmod 33 = 28$

Le message transmis sur le canal est donc C = {26,5,28}

On déchiffre avec la clé privée {7, 33}

- $26^7 \bmod 33 = 5$→ E
- $5^7 \bmod 33 = 14$→ N
- $28^7 \bmod 33 = 19$→ S

Le message déchiffré est bien P = {E;N;S}

Pour le jeu, on limite à p<50 et q<50 et on impose k=5 (donc n > 32)

Le site Dcode [3] permet de calculer des clés publiques et privées,de chiffrer des messages et de craquer des petites clés. Il permet également de voir le temps nécessaire à un PC pour craquer la clé privée à partir de la clé publique. Il faut de très (très) grands nombres pour obtenir un temps significatif.

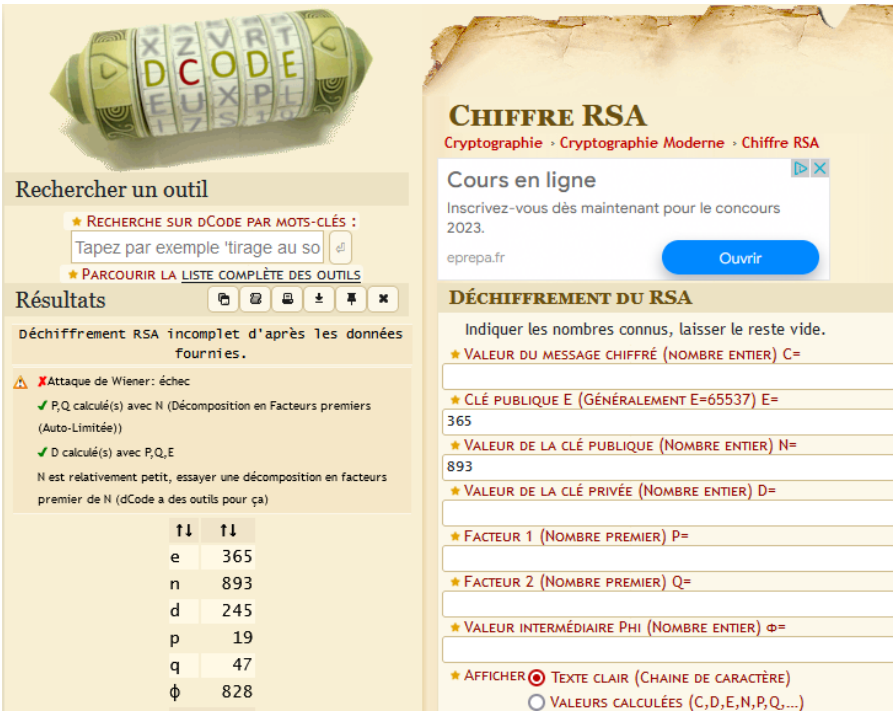


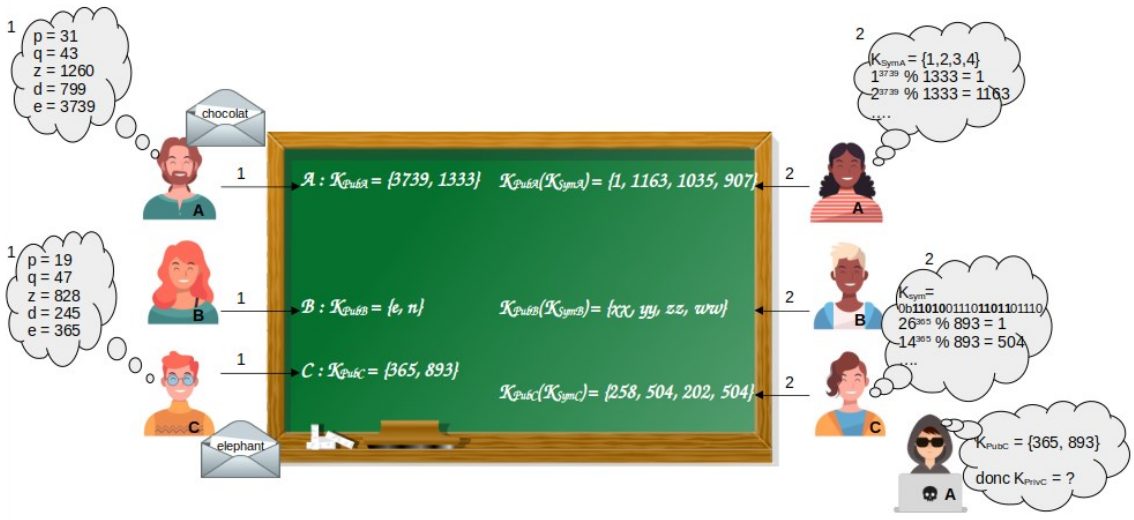
Figure 1 : Copie d'écran du site Dcode > RSA [3]

4 - Déroulement du jeu

Les règles sont expliquées, les étudiants sont répartis entre les chiffreurs d'un côté de la salle avec leur enveloppe et les autres de l'autre côté de la salle.

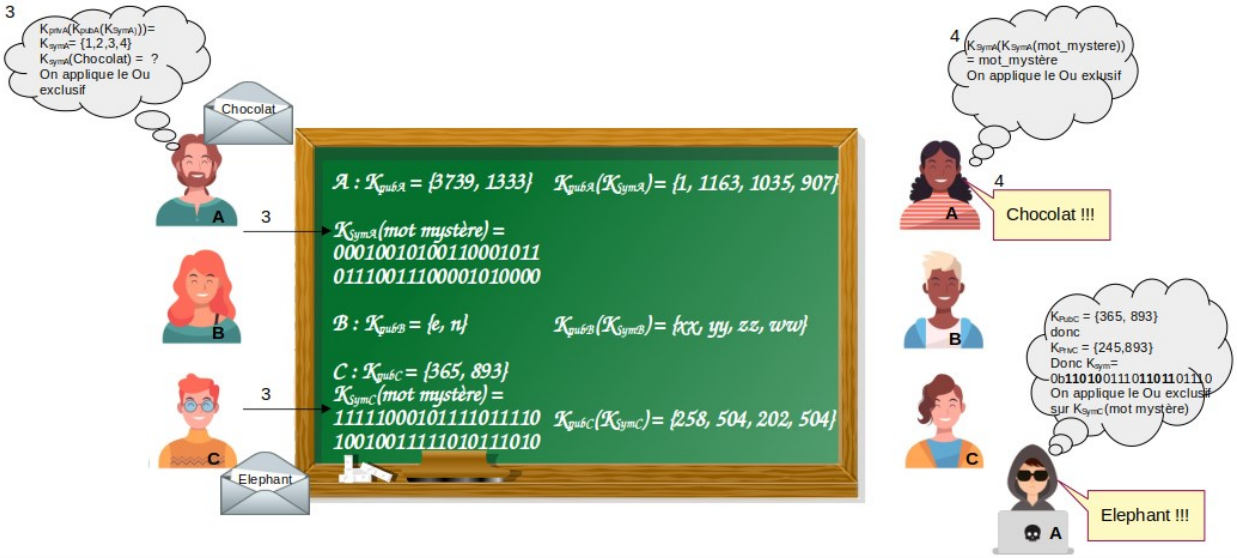
Le tableau est à la vue de tous.

Les chiffreurs doivent trouver un jeu de clés RSA. L'enseignant aide un peu si besoin. Une fois la clé publique obtenue, le chiffreur écrit celle-ci au tableau (1). Les déchiffreurs de son équipe codent alors, avec cette clé publique, la clé symétrique qu'ils ont choisie et écrivent la clé chiffrée au tableau (2). Pendant ce temps les hackeurs des autres équipes cherchent la clé privée pour pouvoir déchiffrer la clé symétrique.



Une fois la clé symétrique chiffrée affichée sur le tableau, le chiffreur la déchiffre avec sa clé privée et l'utilise pour chiffrer le mot mystère puis écrit le mot chiffré au tableau (3). Le déchiffreur utilise la clé symétrique pour déchiffrer le mot mystère et annonce le résultat (4).

Pendant ce temps les hackeurs tentent de trouver les clés privées des chiffrements RSA des autres équipes. S'ils vont suffisamment vite, ils peuvent déchiffrer le message contenant la clé symétrique et ainsi déchiffrer les mots mystère des autres équipes et obtenir leur point.



5 - Conclusion

Les exercices sur les clés symétriques et asymétriques faits pendant le cours, le jeu a duré une petite heure, explication comprise. L'émulation a bien fonctionné, la perspective de gagner quelques chocolats donnant un argument pour tenter de craquer le code de l'équipe adverse. L'équipe A a trouvé le mot A et craqué la clé de l'équipe B, sans avoir le temps de deviner le mot B avant l'équipe B. L'équipe C s'est trompé dans le transfert de sa clé publique et a fini par trouver le mot C avec l'aide de tous. L'enseignant a aidé les uns et les autres pour trouver les clés, chiffrer ou déchiffrer.

Le jeu a permis de mettre en évidence la possibilité de communiquer de manière confidentielle à travers un canal non sécurisé, sans avoir échangé des clés à l'avance. Le fait de s'écarter des ordinateurs a amené les étudiants à prendre la mesure des calculs nécessaires pour le chiffrement symétrique, le chiffrement asymétrique et le craquage d'une clé.

La limite à 50 pour les nombres premiers est sans doute un peu élevée. 40 serait plus raisonnable. Il faudrait peut-être donner une méthode pour trouver d et e.

L'an prochain, un essai d'introduction des certificats avec autorité de confiance est prévu.

Références

[1]: Computer Networks, Andrew Tanenbaum, Nick Feamster, David Wetherall, Pearson Education Limited

[2]: Fondamentaux de la sécurité réseau, M. Sechehaye, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/fondamentaux-dela-securite-reseau

[3]: Dcode, Outil pour déchiffrer/chiffrer avec RSA https://www.dcode.fr/chiffre-rsa

[4]: Cybersécurité, Clés publique/privée, Certificat X509, PKI, Chiffrement RSA, fichier .pem OPC-UA, Hervé Discours, https://www.youtube.com/watch?v=58FUQzWxs3Y

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay

Cybersécurité des systèmes automatisés industriels

La Revue 3E.I
Culture Sciences de l'Ingénieur

Édité le 15/02/2024

école normale supérieure paris—saclay

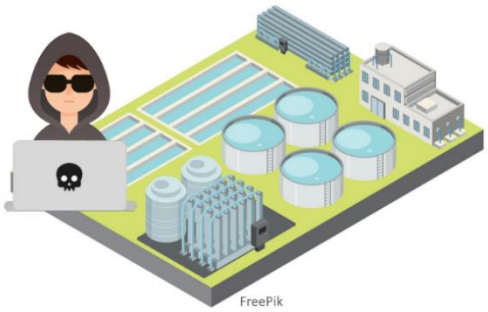
Anthony JUTON[1]

[1] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cet article est une mise à jour l'article publié en juillet 2018 dans la revue 3EI [7]. Il introduit la partie du dossier cybersécurité des systèmes industriels consacrée aux systèmes automatisés. L'automatisme industriel étant essentiellement enseigné en BUT GEII, c'est le public visé par cet article, qui s'efforce de fournir des exemples et des applications pratiques.

Les risques liés à la cybersécurité pour les industries et les services sont réels comme le montre le blocage d'une usine Renault et d'hôpitaux anglais par le ransomware WannaCry en mai 2017 ([3] – Fiche 1). Consciente du risque cyber sur l'industrie et des implications pour le fonctionnement et la sécurité de l'Etat, la loi de programmation militaire de 2013 impose un renforcement de la sécurité informatique à des entreprises privées ou publiques considérées vitales pour la France, regroupées sous le terme Opérateurs d'Importance Vitale (OIV). On trouve notamment parmi les OIV des usines de traitement des eaux, des centrales de production d'énergie, des aéroports, des usines pharmaceutiques.



Ce renforcement concerne l'ensemble des équipements informatiques, ce qui comprend les systèmes gérés habituellement par les services informatiques (IT information technology) normalement sensibilisés à la cybersécurité mais aussi ceux gérés par les services automatisme (OT operational technology), qui doivent se former à ce nouveau risque.

La sécurisation d'une installation industrielle est donc le fruit d'une collaboration entre informaticiens et automaticiens. Cela passe par une implication des informaticiens dans la production et par une formation des automaticiens aux bases de la cybersécurité.

Prenant acte de ce contexte, la licence professionnelle SARII (Systèmes Automatisés Réseaux et Informatique Industrielle) de l'IUT de Cachan (aujourd'hui dissoute dans le BUT3 parcours AII) a créé en 2018 un module de cybersécurité des systèmes industriels pour compléter la formation en automatisme, réseaux et supervision de ses techniciens. Cet article repose essentiellement sur la démarche et les contenus de ce module prévu pour 4h de cours/TD et 12h de TP. L'ensemble s'appuie essentiellement sur les supports proposés par l'Agence Nationale de la Sécurité des

Systèmes d'Information (ANSSI) [1] et par le groupe de travail cybersécurité des systèmes industriels du Club de la Sécurité de l'Information Français (CLUSIF) [2], [3] et [4]. La consultation de ces 4 ressources permettra au lecteur intéressé d'approfondir le sujet.

Dans un premier temps l'article rappelle le risque cyber pour l'industrie, avant d'aborder la démarche proposée par l'ANSSI pour sécuriser un site. L'analyse de quelques incidents récents souligne les bonnes pratiques pour les éviter et l'article termine par une étude de cas d'usine pharmaceutique, support d'une exploitation possible en TD et TP.

1 - L'industrie est soumise à un risque cyber

1.1 - Les types d'attaque

Une attaque peut être ciblée contre l'entreprise (exemple de Stuxnet visant les usines d'enrichissement de l'uranium iraniennes [3] fiche 36 ou de BlackEnergy visant les postes électriques ukrainiens [3] fiche 4) ou non (exemple de WannaCry attaquant tous les systèmes Windows XP ou 7 non mis à jour [3] fiche 1).

L'attaque nécessite une intrusion dans le système (ou dans beaucoup de systèmes extérieurs pour les attaques par déni de service) et un mécanisme de sabotage.

1.1.1 – Solutions pour permettre l'intrusion dans le système

- Un **spyware** ou logiciel espion est un programme qui enregistre les frappes au clavier, webcam, microphone pour récupérer des informations (login et mot de passe notamment). Il peut s'installer lors d'une installation d'un logiciel depuis un site web malveillant, par l'introduction d'un média amovible infecté ou lors de l'ouverture d'un document contenant des macros.
- Le **phishing** ou hameçonnage est un mail utilisant un aspect officiel pour demander la saisie de données personnelles. Plus il est personnalisé (logo de l'entreprise, utilisation de détails concernant la cible), plus il est efficace.
- Un **ver** est un programme qui se reproduit sur plusieurs ordinateurs en utilisant le réseau informatique.

1.1.2 – Mécanisme permettant le sabotage ou la neutralisation du système industriel

- Un **cheval de Troie** est un programme qui permet de prendre à distance le contrôle de l'ordinateur cible. Si un PC de supervision ou de programmation des automates est infecté, le pirate peut modifier dangereusement le comportement du système.
- Un **ransonware** ou cryptovirus est un programme qui chiffre les fichiers et qui demande une rançon pour les déchiffrer. Une fois les fichiers chiffrés, le système est neutralisé.
- Un **virus** est un programme qui s'attache à un autre pour modifier son fonctionnement.
- Le **déni de service** est une attaque qui rend impossible l'utilisation d'un service, notamment via l'utilisation de botnet, réseaux de robots informatiques (souvent installés sur des systèmes informatiques peu protégés) qui vont ensemble saturer un serveur de requêtes.

1.2 - Les opérateurs d'importance vitale

La loi de programmation militaire de 2013 précise les obligations pour 12 secteurs d'opérateurs vitaux pour l'intégrité du territoire de ses habitants ou son économie :

- Activités civiles de l'Etat
- Activités judiciaires
- Activités militaires de l'Etat
- Alimentation
- Communications électroniques, audiovisuel et information
- Energie
- Espace et recherche
- Finances
- Gestion de l'eau
- Industrie
- Santé
- Transports.

Dans ces secteurs, plus de 200 services publics ou entreprises privées dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation sont classés opérateurs d'importance vitale (OIV). La liste est confidentielle, on y trouve des acteurs industriels dans le traitement de l'eau, la production d'électricité, la fabrication de médicaments, la gestion technique des aéroports... La loi impose à ces OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent, nommés « systèmes d'information d'importance vitale » (SIIV).

Les entreprises qui ne sont pas OIV sont également encouragées à prendre des mesures de cybersécurité, ne serait-ce que pour assurer leur survie économique en cas d'attaque.

1.3 - Les spécificités des systèmes industriels

Les systèmes informatiques industriels sont très proches des systèmes informatiques de gestion (utilisation de réseaux Ethernet/TCP/IP, utilisation de PC et serveurs pour la supervision, utilisation de bases de données SQL…) mais ont des spécificités qui les rendent vulnérables et difficiles d'accès aux informaticiens :

- Certains systèmes informatiques industriels (centrales nucléaires, usines en 5x8, aéroports...) doivent être disponibles sans interruptions, rendant difficiles les mises à jour, les tests de vulnérabilité, etc...
- Certains systèmes informatiques industriels mettent en jeu la vie des personnes (centrales nucléaires, machines médicales, usines de production de médicaments…) et pour cela reçoivent des habilitations/qualifications qui ne sont plus valables en cas de mise à jour majeure d'un équipement.
- Les équipements de contrôle-commande ont une durée de vie très longue (on trouve encore en fonctionnement dans les usines de très fiables automates Siemens S5 des années 80) et forment un parc souvent hétérogène (chaque machine peut avoir un modèle d'automate ou pire, une marque d'automate différent). Cela rend le suivi des vulnérabilités et des mises à jour plus fastidieux. Ces automates sont souvent inconnus des informaticiens en charge de la cybersécurité.
- Les productions alimentaires et pharmaceutiques notamment doivent garantir la traçabilité de leur production. Cela rend nécessaire les connexions entre les machines de terrain

(automates, superviseurs, ... regroupés sous le sigle OT Operational Technology) et les machines de l'administration (suivi de la qualité, traçabilité, ... regroupés sous le sigle IT Information Technology).

- Les réseaux de terrain traditionnels (profibus, CANopen, DeviceNet, Modbus RTU...) et certains protocoles TCP/IP largement utilisés en automatisme (Modbus TCP, BACnet/IP, …) ne sont pas sécurisés et pas sécurisables. Ces protocoles sont souvent inconnus des informaticiens en charge de la cybersécurité.
- La maîtrise exigée pour certaines tâches (par exemple la régulation de l'humidité dans des bâtiments d'architecture originale, la mécanique de précision ou l'intégration de robots industriels à des machines automatisées…) demande l'intervention de sous-traitants spécialisés (mécanique, automatisme, robotique, supervision…). A cela s'ajoute la volonté de réduire la masse salariale des entreprises, pratique très présente dans l'automobile. Il est bien sûr plus difficile de maîtriser l'intégrité et la formation en cybersécurité des sous-traitants que celles de ses salariés.

1.4 - Vulnérabilité des systèmes industriels

Pour souligner les vulnérabilités d'un système informatique industriel, voici trois cas représentatifs :

1.4.1 – Système non connecté à Internet

Le système informatique industriel basique comprend typiquement un ou plusieurs automates supervisés par un PC de supervision via un réseau Ethernet, pas forcément connecté à Internet. Un serveur de base de données pour l'archivage peut aussi être présent localement. L'automate contrôle divers équipements via des bus de terrain standard ou basés sur Ethernet.

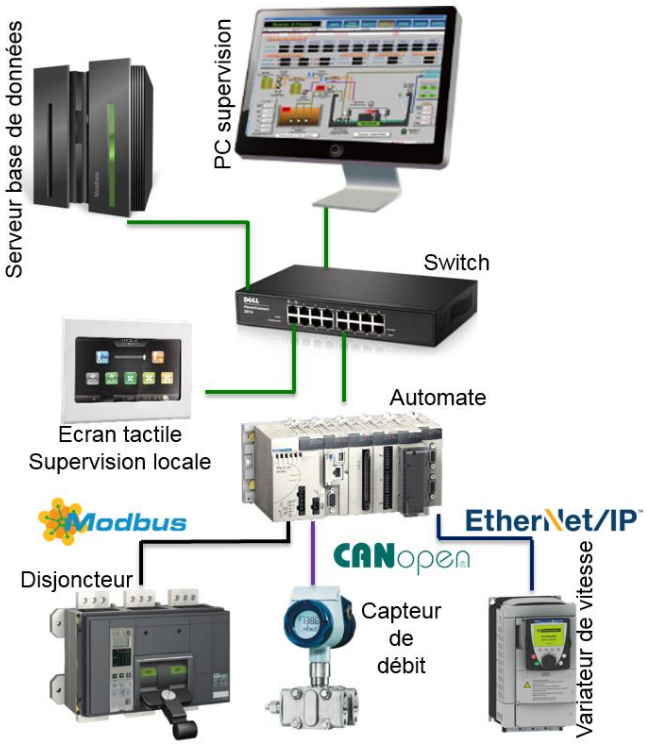


Figure 1 : Architecture type d'un système informatique industriel non connecté à Internet

Les problèmes peuvent survenir de :

- La modification du programme automate via un accès direct à l'automate ou la modification des consignes de supervision par du personnel non autorisé (sous-traitant par exemple),

- L'introduction d'un virus par une clé USB,
- L'introduction d'un virus par un PC maintenance (d'un sous-traitant ou d'un salarié) se connectant au réseau local, pour une mise à jour par exemple.

Le virus peut alors simplement neutraliser le PC de supervision (en chiffrant ses données comme wannacry [3]) ou plus rarement, car beaucoup plus complexe, neutraliser un équipement industriel (automate comme le malware Triton, [3] fiche 7 ou superviseur comme le malware Havex [3] fiche 5) ou plus complexe encore, modifier le programme automate ou les consignes envoyées par le PC de supervision (un seul exemple, Stuxnet [3]).

1.4.2 – Système connecté à Internet

Le réseau de l'atelier est connecté au réseau de l'administration via un routeur. Le réseau de l'administration est lui-même connecté à Internet via un routeur.

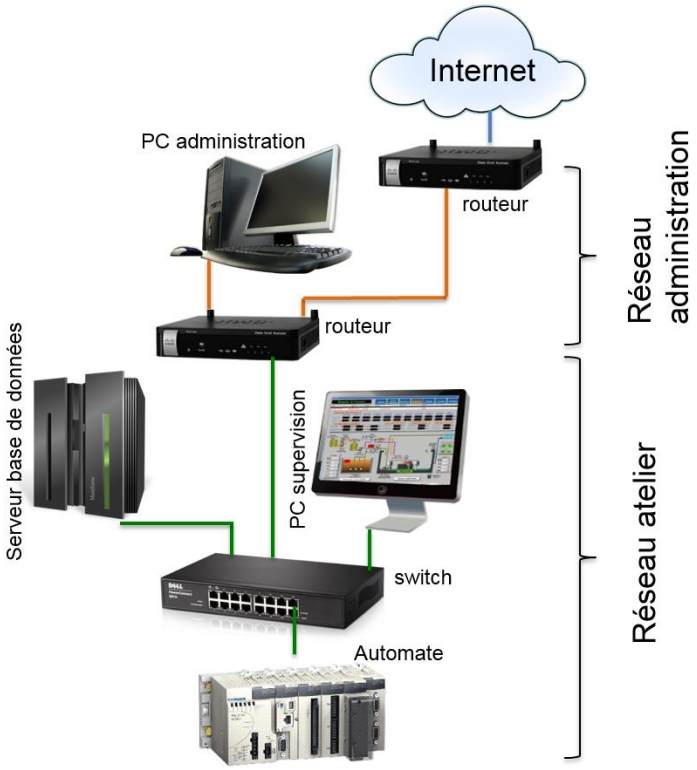


Figure 2 : Architecture type d'un système informatique industriel connecté à Internet

La connexion à Internet, outre une possibilité supplémentaire d'introduction de virus, amène le risque suivant : une personne malveillante peut s'introduire sur le réseau atelier via un accès ouvert (pour la télégestion par exemple) en dérobant des identifiant et mot de passe de connexion ou, plus complexe, via un cheval de Troie installé par un virus sur un PC de bureau par exemple. Cette personne peut alors neutraliser des équipements, les espionner ou en prendre le contrôle à distance.

Tout accès à distance à une installation fait courir le risque d'une prise de contrôle par une personne malveillante. (Exemple de l'attaque d'une station d'épuration, [3] fiche 16, ou [3] fiche 21, parmi beaucoup d'autres)

1.4.3 – Système informatique industriel distribué

Un système distribué désigne un système dont les organes de contrôle-commande (automates, variateurs, modules d'entrées/sorties déportés) ne sont pas localisés dans le même local. Les

grands sites de stockage d'hydrocarbure, les réseaux ferroviaires, les tunnels routiers et les bâtiments en général sont des systèmes distribués.

N'est représentée sur le schéma ci-dessous que la partie contrôle-commande. La supervision et la connexion éventuelle à Internet sont identiques aux architectures présentées ci-dessus.

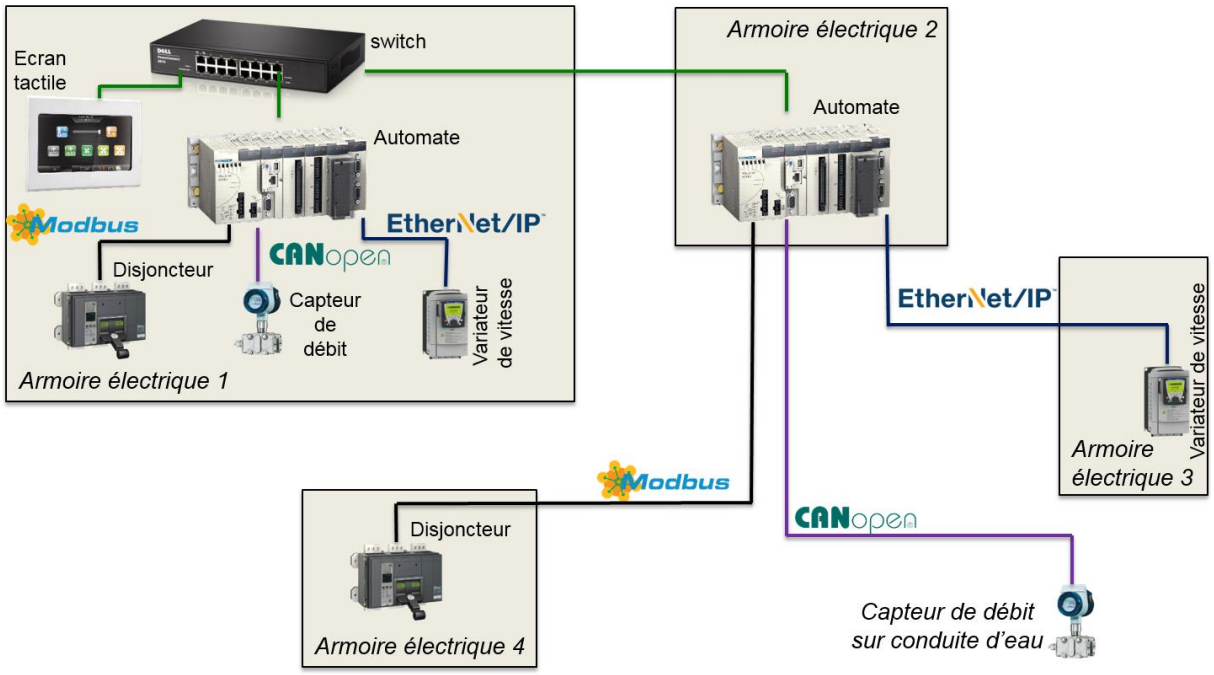


Figure 3 : Architecture type d'un système informatique industriel distribué (partie contrôle/commande uniquement)

Outre les risques précédemment cités, les réseaux de terrain standards, très répandus, très connus dans le monde industriels et très documentés, sur liaison RS485 (Modbus, Profibus, BACnet MSTP), sur bus CAN (CANopen, DeviceNet) ou spécifiques (LON, DALI, KNX…) ne sont pas sécurisés et pas sécurisables simplement (un standard sécurisé de KNX existe mais n'est pas compatible avec les équipements déjà installés). Le passage de ces bus dans des zones publiques ou faciles d'accès fait courir le risque d'une intrusion sur le réseau et de l'envoi sur ce réseau d'informations de capteurs fausses ou de commandes d'actionneurs dangereuses (exemple d'envoi de commande de déversement d'eaux usées en utilisant le réseau industriel local [3] fiche 18 ou exemple de la prise de contrôle d'éoliennes via un accès physique au réseau local [3] fiche 8)

Les réseaux de terrain modernes sur Ethernet (ProfiNet, EtherNet/IP, Ethercat) sont plus récents et leurs standards plus complexes tendent à prendre mieux en compte le risque cyber (authentification de la machine se connectant par exemple). Le protocole OPC-UA, sur Ethernet TCP/IP, utilisé pour la communication entre le superviseur et l'automate, ou entre automates, est même chiffré, ce qui lui donne une popularité certaine actuellement. La ressource [5] traite spécifiquement d'OPC-UA.

2 - Les mesures à appliquer

Une fois les risques présentés, le cours présente alors une version simplifiée de la méthode proposée par l'ANSSI [1] pour la sécurisation des systèmes informatiques industriels et la mise en place d'une politique de sécurité des systèmes d'information (PSSI).

« L'objectif de la Sécurité des Systèmes Informatiques (SSI) est d'étudier les vulnérabilités des systèmes (matériel, logiciel, procédures, aspects humains) afin de déployer des mesures pour les limiter et permettre d'assurer la continuité des fonctions métier à un niveau acceptable. ». Il s'agit

d'assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité du système informatique industriel.

La cybersécurité doit être envisagée par les automaticiens comme la sûreté de fonctionnement des machines :

- On identifie les risques puis la probabilité et les conséquences du risque,
- On met en place des mesures proportionnées au risque (coût et contraintes sur les utilisateurs), sous peine de les voir rejetées.
- On ne peut raisonner en termes de retour sur investissement.

La mise en place de la sécurisation du système informatique industriel doit impliquer les automaticiens, bons connaisseurs de leurs équipements industriels et les responsables cybersécurité de l'informatique générale, formés en cybersécurité mais souvent hermétiques à l'automatisme.

La méthode suit 7 étapes, détaillées ensuite :

1. Sensibilisation des personnels
2. Cartographie des installations et analyse de risque
3. Prévention : concept de la défense en profondeur
4. Surveillance des installations et détection des incidents
5. Traitement des incidents, chaîne d'alerte
6. Veille sur les menaces et les vulnérabilités
7. Plans de reprise et de continuité d'activité

La méthode ne fait appel qu'à des compétences d'automaticien moderne (les compétences en réseaux sont évidemment importantes). Elle montre que la cybersécurité est surtout une question d'organisation et de temps alloué à cette organisation, d'où l'obligation d'un PSSI pour les OIV.

2.1 - Sensibilisation des personnels

La majorité des incidents est liée à l'imprudence des personnels de l'entreprise :

- Utilisation de clé USB,
- Logiciel « cheval de Troie » ou virus installés en ouvrant un fichier ou en installant un logiciel de provenance douteuse,
- Divulgation de ses identifiant/mot de passe en réponse à un mail de phishing,
- Mot de passe écrit sur un post-it ou stocké en clair sur une machine,
- Identifiant/mot de passe identique pour tous les techniciens (y compris ceux qui quittent l'entreprise…),
- Machines non protégées ou avec les identifiant/mot de passe par défaut, avec des mises à jour logicielles non effectuées.

Plus de 10 fiches « incident » du Clusif [3] ont pour origine un vol de mot de passe par une campagne de phishing, plusieurs autres ont un lien aussi avec des manquements à la sécurité des employés (non révocation des accès d'un employé licencié, installation de logiciel infecté...)

La sensibilisation de tous les personnels aux règles d'« hygiène informatique » contribue à réduire fortement les vulnérabilités et les opportunités d'attaques. La sensibilisation doit être régulière car les risques évoluent en permanence et les mauvaises pratiques reviennent.

2.2 - Cartographie des installations et analyse de risque

Comme pour la sécurité des machines, la seconde étape est un audit de l'installation :

- Quels sont les objectifs métier (production, distribution, protection des biens et des personnes…) et les services assurés ?
- Quels sont les impacts en cas d'interruption de service ? En cas de modification du comportement du système ?
- Quelles sont les fonctions indispensables à l'atteinte des objectifs, et en particulier :
  - leurs niveaux d'implication et de criticité dans la réalisation des services,
  - les systèmes qui les portent,
  - si ces systèmes sont centralisés, distribués, accessibles à distance, etc.

Cela amène donc à un inventaire des installations matérielles (référence de l'équipement, version, protections, accès), de l'architecture réseau et des communications entre les équipements internes et externes. Cela amène également à séparer les équipements critiques devant être très protégés des autres. Les plus critiques, systèmes d'information d'importance vitale (SIIV), doivent être déclarés à l'ANSSI.

L'ANSSI propose une méthode d'analyse du risque nommée EBIOS [1].

2.3 - Prévention : concept de la défense en profondeur

On entre ici dans la partie technique de la cybersécurité : la défense en profondeur consiste à protéger les installations en les entourant de plusieurs barrières de protection autonomes et successives, de sorte d'assurer la protection même en cas de compromission d'un équipement. Ces barrières peuvent être technologiques ou liées à des procédures organisationnelles ou humaines.

Première règle : tout est interdit par défaut. On autorise juste les accès nécessaires aux personnes concernées, on n'ouvre que les connexions UDP/TCP utiles, on n'installe que les logiciels indispensables.

Voici les protections à mettre en place :

- **Protection physique** : c'est la protection la plus simple, les équipements de contrôle-commande doivent être dans des armoires fermées à clé, le local de supervision ne doit être accessible qu'aux personnes autorisées. Siemens propose par exemple des verrous bloquant l'accès aux ports Ethernet des équipements (automates, switch...).

Figure 4 : Verrou Siemens pour prise RJ45 : IE RJ 45 Port Lock

- **Pare-feu** : sur les routeurs et sur les Pcs et automates, on bloque les ports UDP et/ou TCP non utilisés pour empêcher les requêtes indésirables d'arriver jusqu'à la machine. Les pare-feux avancés permettent de faire de l'inspection de paquets en profondeur (le pare-feu vérifie que le contenu d'un paquet arrivant sur le port 502, dédié à Modbus, est bien une requête Modbus par exemple).
- **Cloisonnement des réseaux**, notamment pour séparer le réseau industriel (OT) du réseau de l'administration (IT) : Les VLANs et les pare-feux des routeurs permettent de filtrer les échanges entre un sous-réseau et un autre. On veillera notamment à n'autoriser que les requêtes indispensables à entrer dans le sous-réseau atelier. Il est possible d'installer des **diodes réseau** (les informations ne passent physiquement que dans une direction, ce qui interdit les communications TCP) ou passerelles unidirectionnelles (un peu plus avancées, elles acceptent les établissements de connexion TCP et les acquittements, pour permettre un flux d'information TCP dans une seule direction).
  Il est possible également de mettre une **passerelle de rupture protocolaire**. Celle-ci, en passant le message d'un protocole de communication à l'autre, permet d'éviter l'exploitation de failles dans un des protocoles.
- **Protection antivirale**, les PCs (supervision, programmation) doivent avoir un antivirus à jour. Une procédure explicite de mise à jour des antivirus doit exister.
- **Durcissement des configurations** :

  Pour un PC de supervision :

  - Ne garder que les logiciels indispensables à la supervision (pas de logiciel de programmation des automates, pas de navigateur web, pas de logiciels de bureautique…) ;
  - Bloquer les médias amovibles (clés USB) sur les ports usb ;
  - Mettre un mot de passe sur le Bios pour notamment empêcher un démarrage sur un autre support que le disque de la machine ;
  - Supprimer ou désactiver les fonctions non utilisées mais activées par défaut.
  - Mettre à jour le système d'exploitation et le logiciel de supervision. Il peut être nécessaire pour cela d'avoir une installation miroir réduite pour tester les mises à jour avant leur mise en production ;
  - Distinguer clairement les profils (OS et supervision) utilisateur et administrateur. Le PC de supervision est sur un profil utilisateur (pas de droit pour installer des logiciels) et chacun dispose sur la supervision d'un profil adapté à ses besoins. Chaque personne a des identifiant/mot de passe uniques ;
  - Choisir un logiciel de supervision offrant les meilleures caractéristiques pour répondre aux exigences de sécurité et mettre en place ces fonctionnalités : mécanismes d'authentification, ségrégation des droits (la personne chargée de la maintenance peut acquitter les alarmes mais ne peut modifier les consignes du système par exemple) ;
  - Les logiciels de programmation des automates sont sur des PCs éteints et stockés sous clé ;

  Sur les automates :

  - Changer les configurations par défaut (mot de passe par exemple),
  - Mettre à jour régulièrement le firmware de l'automate (disponible sur le site du fabricant),
  - Supprimer ou désactiver les fonctions non utilisées mais activées par défaut (serveur web, utile pour la configuration mais pas pour l'utilisation, serveur FTP...).

Dans ce cadre de défense en profondeur, des procédures accompagnent ces défenses techniques, notamment concernant les interventions des sous-traitants qui doivent être planifiées précisément (mots de passe, accès, utilisation de ses propres outils ou non, échanges de matériels, qualifications…). L'ANSSI publie un guide de l'externalisation pour accompagner les entreprises dans la mise en place des procédures d'intervention des sous-traitants.

2.4 - Surveillance des installations et détection des incidents

Les équipements réseaux proposent des journaux et pour les plus avancés des alarmes permettant d'indiquer un trafic anormal. Surveiller le réseau en lisant ces journaux système et en configurant ces alarmes mais aussi en formant le personnel à détecter et signaler des comportements suspects de leur machine n'empêchera pas un incident mais permettra de le détecter au plus tôt et d'en limiter autant que possible les effets.

Plus un incident sera détecté tôt, plus il sera possible de mettre en place des mesures pour en réduire et confiner les effets comme par exemple :

- Isoler physiquement les installations en cas d'attaque virale pour limiter les risques de propagation (on déconnecte du réseau les machines),
- Arrêter une installation avant sa dégradation si des données de configuration ne sont plus intègres.

2.5 - Traitement des incidents, chaîne d'alerte

Le dispositif de détection des incidents est associé à une organisation et des procédures pour traiter les incidents :

- Que faire lors de la détection d'un incident ?
- Qui alerter ?
- Quelles sont les premières mesures à appliquer ?

La gestion des incidents doit également intégrer une phase d'analyse post incident qui permettra d'améliorer l'efficacité des mesures déployées initialement.

2.6 - Veille sur les menaces et les vulnérabilités

La sécurité informatique est une action continue nécessitant des efforts permanents (on revient à l'importance du PSSI). La ou les personnes en charge de la cybersécurité du système industriel doivent mettre en place une organisation pour :

- Se tenir informés de l'évolution des menaces, des vulnérabilités, sur le site Internet de l'ANSSI ([1] et [6]) et sur celui des équipementiers qui doivent indiquer les vulnérabilités et les mises à jour disponibles de préférence via des envois d'alerte sécurité.
- Mettre à jour régulièrement les micrologiciels (firmwares) des automates et autres équipements (variateurs, écrans tactiles…) et les systèmes d'exploitation et les applications des PCs de supervision et autres serveurs de bases de données. Comme indiqué précédemment, cela peut nécessiter d'avoir une installation miroir réduite pour les tests de ces mises à jour avant leur mise en production.

L'entreprise doit donc accepter un coût et une période de maintenance pour ces mises à jour et les tests associés. La mise à jour doit parfois passer par la migration d'un OS non maintenu à sa version suivante. Précisément, Windows XP n'étant plus maintenu, il ne devrait plus être utilisé sur

des systèmes industriels critiques. Wannacry a mis en évidence la vulnérabilité de Windows XP et le coût potentiel de sa conservation. (Le coût de Wannacry qui exploitait une faille connue de XP a été estimé entre 1 et 4 Milliards de dollars par différentes agences nationales de sécurité informatique).

Pour les systèmes qualifiés avec des versions d'un firmware et d'un système d'exploitation, il est nécessaire lors de la conception du projet, de prendre en compte la mise à jour des firmwares des automates et des logiciels de supervision et systèmes d'exploitation et d'intégrer des mécanismes de requalification des équipements si besoin. Si ce n'est pas possible (système ancien), le système doit être isolé du réseau avec uniquement des communications précises, surveillées et unidirectionnelles vers le réseau.

2.7 - Les plans de reprise et de continuité

L'objectif du plan de reprise est de se préparer à faire face à des événements exceptionnels pour lesquels toutes les mesures précédentes auraient échoué afin de minimiser les impacts et permettre de redémarrer l'activité le plus rapidement possible.

Il est important pour cela de disposer d'une sauvegarde de chaque automate, des équipements réseau et du PC de supervision, des codes sources et des données et de prévoir des modes de fonctionnement dégradé (le système continue la production, mais moins vite ou avec plus d'interventions manuelles). Les sauvegardes doivent être stockées sur des supports amovibles ou sur des machines éteintes ou déconnectées du réseau (sauvegardes froides).

Pour des systèmes critiques, on prévoira un approvisionnement (automates, PC) pour limiter la durée de l'arrêt de la machine.

3 - Analyse d'incidents

La méthode décrite, le cours reprend à partir des fiches du CLUSIF [3] avec 4 incidents de cybersécurité et invite les étudiants à chercher quelle vulnérabilité a été exploitée et quelle étape de la méthode aurait pu empêcher une telle attaque :

- Fiche 16 : Attaque d'une station d'épuration des eaux
- Fiche 19 : Empoisonnement de l'eau potable
- Fiche 32 : Prise de contrôle du système de production d'une aciérie
- Fiche 4 : Coupure générale d'électricité - BlackEnergy

Ces 4 études de cas montrent qu'à chaque fois, ce sont 2 failles successives qui ont permis l'attaque. La mise en place de la méthode de sécurisation des installations, assez accessible, aurait permis de les éviter.

Les fiches étant bien détaillées, le lecteur pourra s'y référer pour organiser une activité similaire, et y puiser d'autres exemples.

4 - Étude de cas pratique

Le cours de cybersécurité termine par une étude de cas fictive de sécurisation d'un site OIV associé à sa mise en œuvre en Travaux Pratiques sur 12h.

Le contexte : on considère une usine pharmaceutique française disposant d'un atelier de fabrication et d'un atelier d'emballage. L'usine produisant de l'insuline (nécessaire aux personnes

diabétiques), elle est classée Opérateur d'Importance Vitale (OIV). De plus, la réglementation pharmaceutique exige une traçabilité importante de la qualité de la production. Le siège de l'entreprise situé au Danemark héberge la base de données comprenant les autorisations d'accès et doit pouvoir récupérer les données de production de l'usine française.

La supervision des deux ateliers a lieu dans un local de supervision situé dans l'atelier. La supervision, outre l'affichage des informations sur le système (mesures, alarmes… utilisées par les services maintenance et qualité), permet au chef d'atelier de passer certaines machines en mode manuel et de modifier les cadences, notamment pour adapter le débit de la production à celui de l'emballage.

Pour travailler en salle de TP, les IP publiques des routeurs site sont remplacées par des IP du sous-réseau 192.168.2.0/24, qui joue le rôle de réseau « public » de la salle de TPs. Une connexion sécurisée VPN relie le site Danois et le site Français.

L'installation est donc la suivante lors de l'arrivée des étudiants « sur site » :

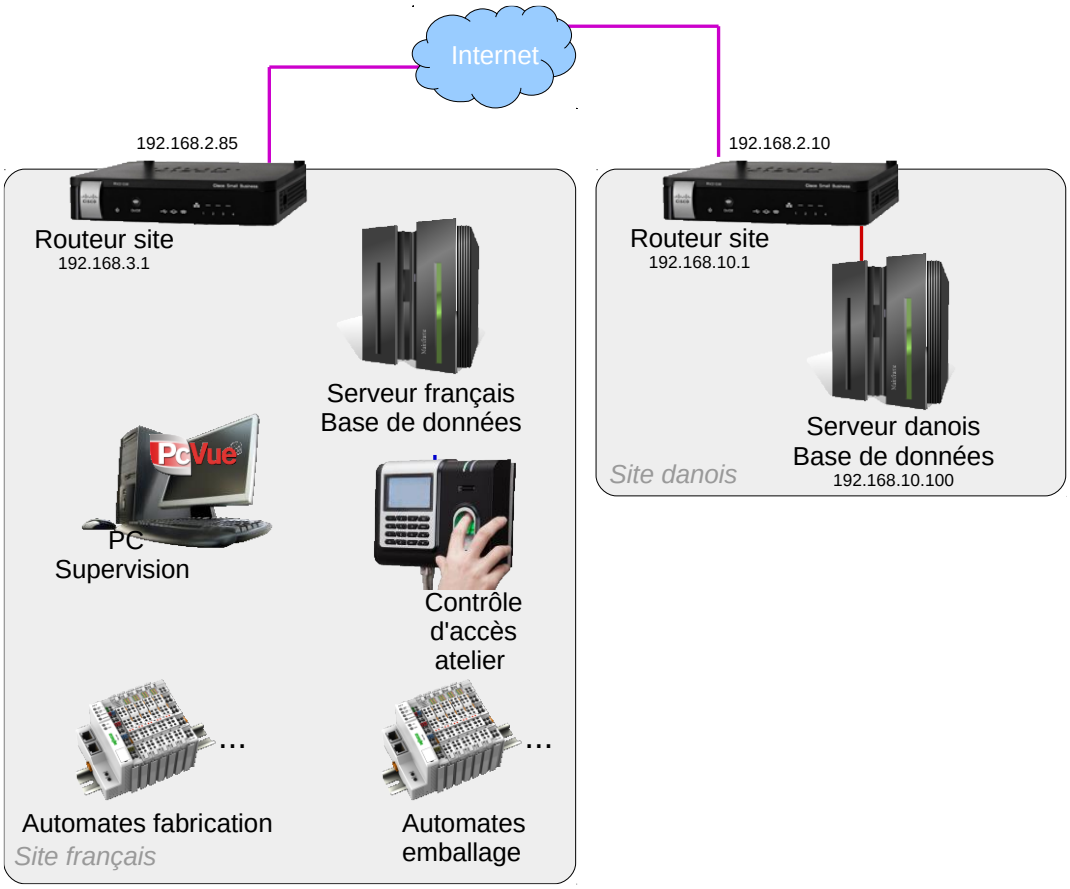


Figure 5 : Equipements de l'entreprise de production avant sécurisation du site

Tout d'abord, les étudiants mettent en place la connexion sécurisée VPN site-à-site entre les 2 routeurs (Cisco RV215W).

Ensuite, les étudiants mettent en place une supervision simplifiée : une entrée Tout ou Rien de l'automate de fabrication remonte à la supervision en modbus TCP. Celle-ci contrôle également une sortie Tout ou Rien de ce même automate.

Les étudiants demandent ensuite au superviseur PCVue le stockage des valeurs de l'entrée et de la sortie de l'automate dans le serveur de base de données SQLServer (requête SQL passant sur TCP/IP).

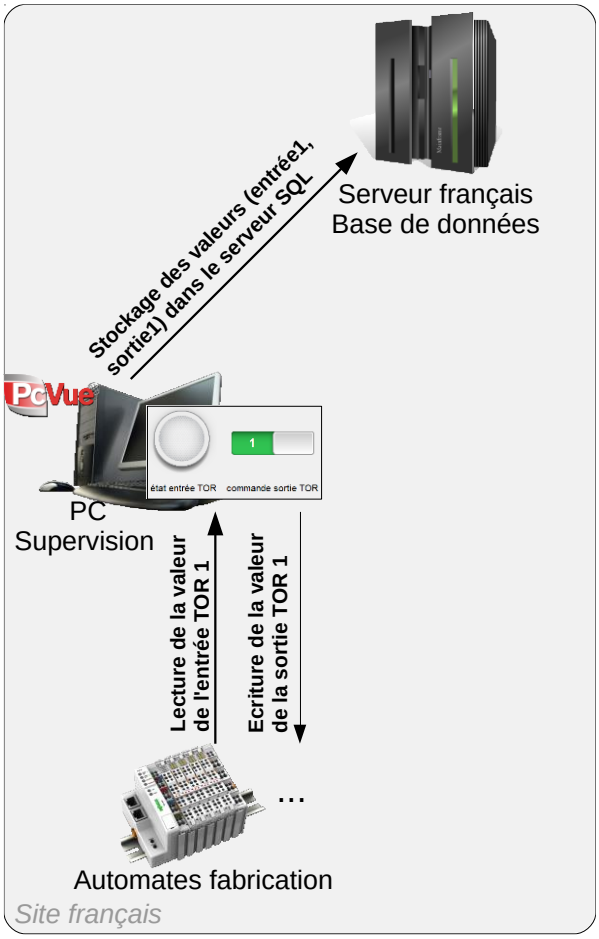


Figure 6 : Echanges entre les équipements du site français

On reprend alors à travers ce TP les différentes étapes de la méthode pour sécuriser un site :

4.1 - Sensibilisation des personnels

Les étudiants doivent expliquer rapidement la mise en place d'une politique de sensibilisation des personnels à la sécurité du site et à la cybersécurité, en insistant notamment sur le phishing, les clés USB, les fichiers douteux, le choix et le non stockage des mots de passe et l'alerte à donner en cas de détection d'un comportement suspect de machine.

4.2 - Cartographie des installations et analyse du risque

Le site étant d'importance vitale et un contrôle à distance non nécessaire (un chef de production est toujours présent sur le site), l'analyse du risque amène à choisir de bloquer tous les accès entrants dans l'atelier.

Les données de traçabilité doivent tout de même être disponibles pour les Danois. Elles seront partagées via un serveur SQL situé à l'extérieur de l'atelier, dans une DMZ. Une DMZ (zone démilitarisée, en référence à la zone « neutre » servant notamment pour l'échange de prisonniers entre les 2 Corées) est un sous-réseau du site accessible depuis l'extérieur et depuis les sous-réseaux sensibles du site (ici, l'atelier). Il n'est pas possible d'accéder au réseau atelier depuis la DMZ. Les équipements des sous-réseaux sensibles y déposent les données que les équipements extérieurs viendront y chercher, sans avoir besoin d'entrer dans le sous-réseau sensible.

Les données pourraient aussi, en plus, être stockées localement sur le PC de supervision (ou sur un serveur SQL dans l'atelier) si l'on voulait être sûr de les conserver en cas d'attaque. Pour tenir en 12h, ce dernier point n'est pas retenu.

Dans les ateliers, l'isolation des réseaux amène à un VLAN et sous-réseau par atelier (192.168.4.0/24 pour la fabrication et 192.168.5.0/24 pour l'emballage) et un VLAN et sous-réseau (192.168.6.0/24) pour le contrôle d'accès du bâtiment. Ainsi, l'infection d'une machine aura plus de mal à se propager d'un atelier à un autre, les zones de diffusion étant segmentées. Le PC de supervision doit communiquer avec les deux VLANs des ateliers. Pour cela, soit sa carte de réseau accepte les VLANs tagués et est rattachée aux 2 VLANs ateliers, avec 2 IP, soit on met 2 cartes réseaux dans le PC de supervision chacune attachée à un VLAN avec une IP dans le sous-réseau associé.

La cartographie des installations et l'analyse du risque amènent les étudiants à proposer l'architecture réseau suivante :

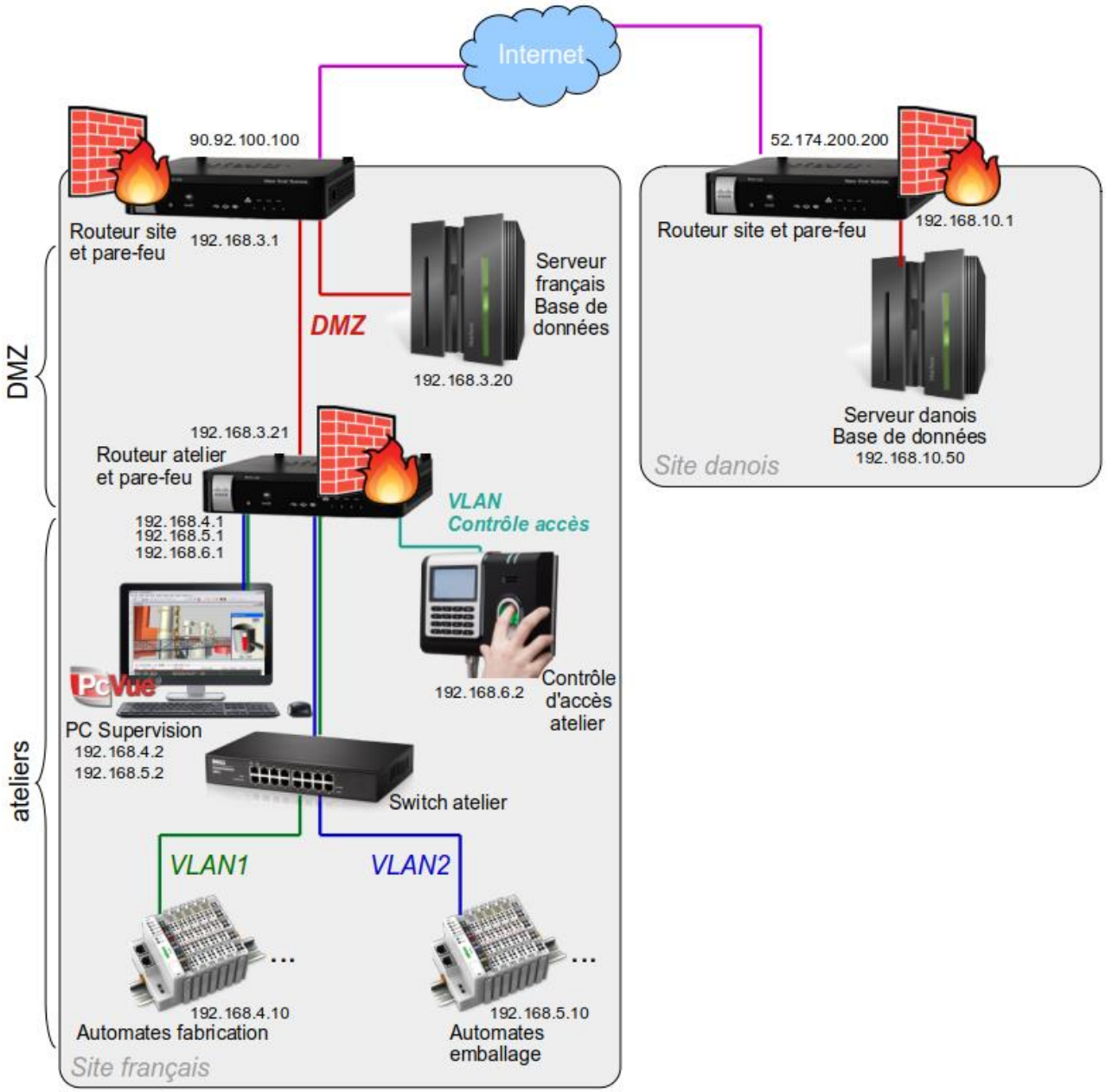


Figure 7 : Architecture réseau de l'entreprise de production de médicaments

4.3 - Prévention : défense en profondeur

Les étudiants câblent leur réseau et abordent alors les différents aspects de la défense en profondeur de l'installation.

4.3.1 – protection physique des équipements

Les étudiants doivent indiquer les mesures de protection physique minimales : armoires électriques et réseaux sous clés, accès à l'atelier et au local de supervision soumis à un contrôle d'accès strict, suppression des accès des employés ayant quitté l'entreprise.

4.3.2 – Cloisonnement des réseaux et durcissement de leur configuration

Les étudiants configurent les pare-feux :

- Le routeur atelier refuse toutes les requêtes entrantes (fonctionnement en passerelle unidirectionnelle) et n'accepte que les requêtes sortantes du PC de supervision vers le port 1433 du serveur SQL.
- Le routeur site français refuse également les requêtes entrantes. Il est configuré en VPN site-à-site avec le routeur site danois, ce qui permet un accès au serveur de base de données français par le serveur danois.

Sur les serveurs de base de données (des PCs équipées de SQL Server Express), SQL Management Studio Express sert de client SQL permettant de lire dans une base de données locale ou distante.

4.3.3 – Durcissement du PC de supervision

Sur le PC de supervision, sur lequel les étudiants sont administrateurs :

- Vérification de l'activation du firewall du PC,
- Établissement d'un identifiant/mot de passe pour chaque utilisateur (le chef d'atelier et le technicien de maintenance) avec des droits limités (pas de possibilité d'installation de logiciels et pas de possibilité de modifier la configuration réseau),
- Établissement également d'une ségrégation des droits sous PCVue. Le chef d'atelier a les droits pour modifier la variable de sortie de l'automate. Le technicien de maintenance peut juste observer les variables,
- Blocage des médias amovibles usb : blocage de la détection des périphériques de stockage USB, désactivation du pilote de gestion des périphériques de stockage USB, désactivation de l'exécution automatique, en suivant la procédure proposée sur le site de l'ANSSI.
- Indication du fait qu'il faudrait supprimer les logiciels autres que le superviseur PCVue du PC, en particulier les logiciels de programmation des automates, très dangereux (ils permettraient à une personne prenant le contrôle du PC de supervision de modifier les programmes de production des médicaments), et les logiciels de bureautique, très attaqués.
- Le PC de supervision étant client des automates serveurs et client SQL, son pare-feu doit être configuré pour ne pas accepter les requêtes entrantes. C'est la configuration par défaut du pare-feu windows. On peut vérifier qu'elle est correcte et que le pare-feu est bien activé au lancement du PC (Menu Sécurité Windows des paramètres de la machine)

4.3.4 – Durcissement des automates

Les étudiants récupèrent le firmware à jour chez le fabricant et le chargent dans les automates.

Ils désactivent le serveur web embarqué de l'automate. Les serveurs web embarqués sont très utilisés pour la configuration des équipements industriels mais sont vulnérables car utilisant des technologies web standard (parfois anciennes, les automates ayant une longue durée de vie).

4.4 - Surveillance des installations et détection des

- Les étudiants utilisent le port mirroring du routeur site et Wireshark (avec des filtres bien choisis) pour surveiller les échanges réseaux. Ils peuvent vérifier que les trames extérieures au site sont bien chiffrées (protocole ESP) et détecter les incidents ;

	Time	Source	Destination	Protocol	Length	Info
379	17.166214	192.168.2.10	192.168.2.85	ESP	310	ESP (SPI=0x51d0f1a7)
380	17.173467	192.168.10.100	192.168.3.102	TDS	246	SQL batch
381	17.174008	192.168.3.102	192.168.10.100	TDS	142	Response
382	17.175583	192.168.2.85	192.168.2.10	ESP	214	ESP (SPI=0x11bfd739)

```
Frame 379: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface 0
Ethernet II, Src: Cisco_aa:c7:24 (10:bd:18:aa:c7:24), Dst: Cisco_ab:c6:99 (10:bd:18:ab:c6:99)
Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.2.85
Encapsulating Security Payload
```

```
Frame 380: 246 bytes on wire (1968 bits), 246 bytes captured (1968 bits) on interface 0
Ethernet II, Src: Cisco_ab:c6:98 (10:bd:18:ab:c6:98), Dst: Dell_04:14:53 (d8:9e:f3:04:14:53)
Internet Protocol Version 4, Src: 192.168.10.100, Dst: 192.168.3.102
Transmission Control Protocol, Src Port: 4854, Dst Port: 1433, Seq: 20248, Ack: 7069, Len: 192
Tabular Data Stream
```

Figure 8 : Surveillance des échanges au niveau du routeur site

- Les étudiants ouvrent les journaux du routeur pour connaître l'historique des connexions VPN ;
- Les étudiants ouvrent les journaux du serveur SQL (accessibles par SQL Management Studio) pour connaître l'historique des connexions au serveur SQL.

4.5 - Traitement des incidents, chaîne d'alerte

Les étudiants proposent une procédure en cas de virus sur le serveur SQL : mise en place d'un archivage (archivage obligatoire pour la traçabilité de la fabrication de médicaments) local par exemple en attendant la remise en état du serveur SQL.

4.6 - Veille sur les menaces et les vulnérabilités

Les étudiants proposent un plan de veille sur les mises à jour de sécurité du fabricant des automates, de Windows et de PCVue.

4.7 - Les plans de reprise et de continuité d'activité

Les étudiants sauvegardent les programmes automates, l'application de supervision et les configurations des 2 routeurs sur un dossier qu'ils expliquent devoir garder sous clé sur une machine ou un support non connecté au réseau.

5 - Étude de cas simulée

Période propice aux discussions sur l'importance vitale de l'industrie pharmaceutique, mai 2020 a amené à faire le TP cybersécurité à distance. Cisco Packet Tracer permet de travailler sur la configuration des équipements réseaux (VPN, pare-feu, VLAN, DMZ), sans toutefois apporter l'ensemble des savoir-faire d'un véritable TP : programmation du superviseur, ségrégation des droits, configuration des restrictions sur les PCs, mise à jour des automates, mise en place des requêtes SQL…

Le fichier pkt « professeur » est donné à titre indicatif en pièce jointe à cette ressource. Toutes les fonctionnalités n'ont pas été testées.

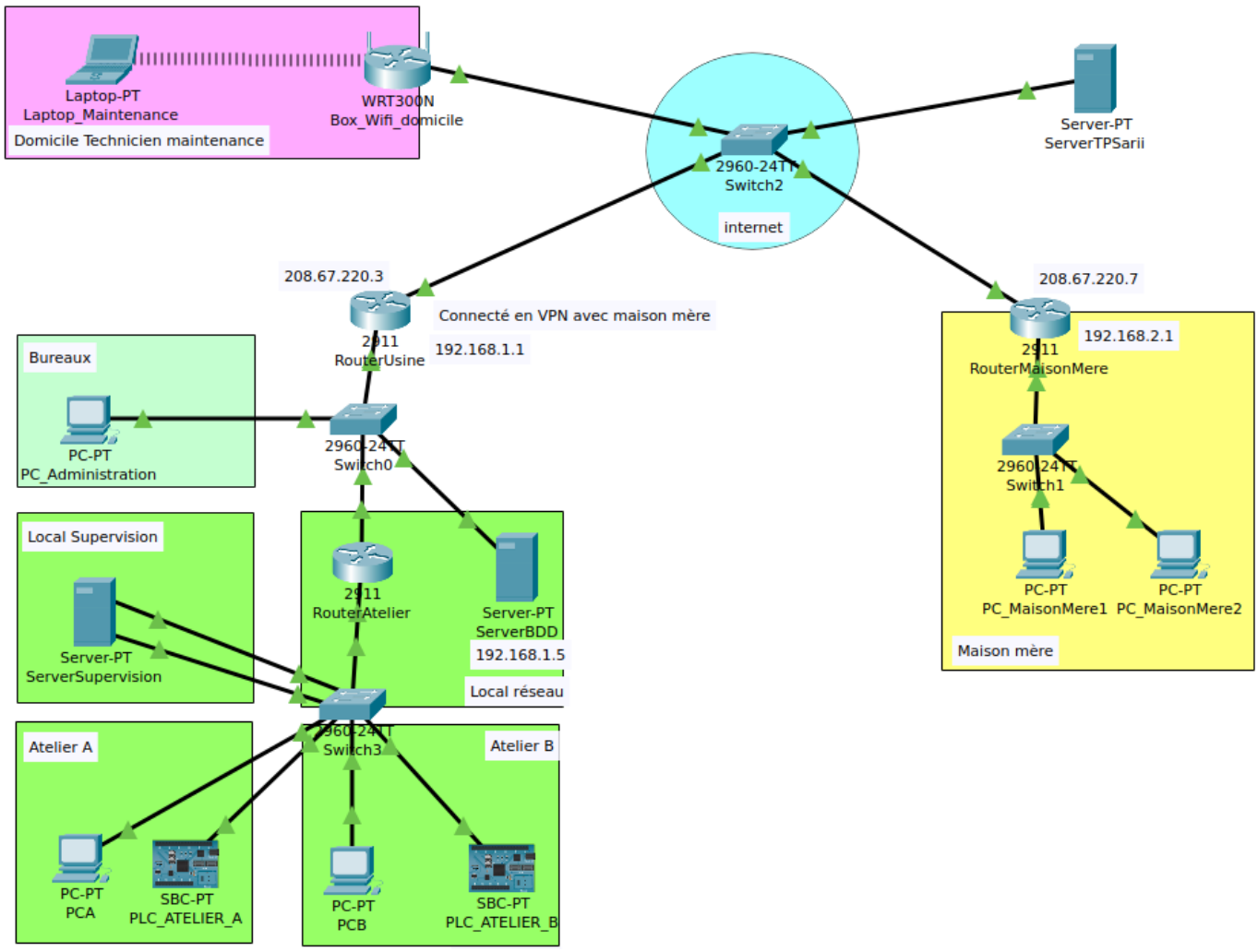


Figure 9 : copie d'écran de l'installation pharmaceutique sous cisco packet tracer

6 - Conclusion

Le cours et le TP cybersécurité des systèmes automatisés industriels permettent aux étudiants d'être sensibilisés au risque cyber, de connaître les principales mesures à mettre en place pour sécuriser un site. Cette séquence pédagogique leur fait prendre conscience que ces mesures, à leur portée, permettent de contrer la plupart des attaques ciblées ou non contre un réseau informatique industriel.

Ce cours/TP est à compléter par la présentation et l'exploitation du protocole sécurisé OPC-UA, pris en compte par les automates industriels modernes (Siemens S7-1500, Schneider M251 par exemple) et objet d'une seconde ressource de ce dossier [5].

Références :

[1]: ANSSI : Publications sur la cybersécurité des systèmes industriels
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

[2]: Guide Cybersécurité des systèmes industriels, Clusif, 2021
https://clusif.fr/publications/guide-cybersecurite-des-systemes-industriels-2021/

[3]: Fiches incidents cyber si industriels, Clusif, 2022
https://clusif.fr/publications/fiches-incidents-cyber-si-industriels/

[4]: Panorama des référentiels - Cybersécurité des systèmes industriels
https://clusif.fr/publications/panorama-des-referentiels-2eme-edition-2/

[5]: OPC UA, un protocole sécurisé pour l'automatisme industriel (à paraître)

[6]: ANSSI – CERT-FR : Centre Gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. https://www.cert.ssi.gouv.fr/

[7]: La Revue 3EI – N°93 - juillet 2018 : Cyber-sécurité et réseau électrique,
https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/3ei-n93-juillet2018-cybersecurite-et-reseau-electrique

La Cybersécurité chez Eiffage Energie Systèmes

La Revue 3E.I
Culture Sciences de l'Ingénieur

Édité le 01/02/2024

école normale supérieure paris—saclay

Jocelyn ZINDY[1] – Franck LE GALL[2]

[1] *Eiffage Energie Systèmes,* [2] *ISEN Brest*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cet article est issu d'un entretien avec M. Zindy, directeur du développement commercial Cybersécurité - Industries du Futur de Eiffage Energie Systèmes. Il présente d'une part le cadre général de la Cybersécurité dans le domaine de l'OT (Operational Technology) en précisant les spécificités de l'OT vis-à-vis de l'IT et d'autre part comment un grand groupe comme Eiffage intègre celle-ci dans ses offres.

1 - Introduction

Les cyberattaques sont devenues monnaie courante dans nos sociétés modernes. Elles touchent les réseaux internet, mobiles, Wifi et les systèmes qui leurs sont connectés. On pense en premier lieu aux ordinateurs et à tout l'univers de l'IT (Information Technology) mais cette menace est aussi bien réelle pour le monde industriel. Les grandes entreprises du domaine sont particulièrement attentives à ces évolutions et proposent des solutions pour y remédier.

Le groupe Eiffage exerce dans de nombreux domaines : construction, infrastructures, concessions et énergie. Il s'agit du troisième groupe de constructions et de concessions français, derrière Vinci et Bouygues, et du quatrième groupe européen. En 2023, il comprend plus de 70 000 collaborateurs. C'est dans la branche « Energie systèmes » qui compte environ 29 000 personnes que travaillent une trentaine d'experts en cybersécurité.

Dans le monde de la cybersécurité, Eiffage Energie Systèmes n'est ni un « pure player », ni spécialisé dans la cybersécurité IT, il reste proche de son cœur de métier en offrant un volet cybersécurité dans le domaine de l'OT (Operational Technology). En tant qu'intégrateur multi technologies, il propose à ses clients de répondre aux clauses de cybersécurité qui sont maintenant présentes dans les appels d'offre.

Il existe de nombreuses entreprises qui proposent des solutions de cybersécurité. On peut citer Atos ou Sopra Steria qui bien que très majoritairement orientées vers l'IT (environ 95%) réalisent aussi des prestations orientées OT (environ 5%). D'autres acteurs de plus petite taille (quelques dizaines de personnes), sont des « pure players » c'est-à-dire des petites entreprises spécialisées dans la cybersécurité OT.

Figure 1 : La cybersécurité dans l'Operational Technology

2 - OT versus IT

Qu'est que l'OT ? Nous sommes habitués à entendre parler de l'IT qui est exploité au sein des systèmes d'information d'entreprise alors que l'OT est mise en œuvre pour la gestion et la prise en charge des systèmes d'Information Industriels ou techniques. Alors que l'IT concerne principalement les réseaux, les logiciels, la téléphonie, c'est à dire la gestion de l'entreprise, l'OT est plus proche des process et prend en compte les automates, les capteurs …. Le marché de la cybersécurité se réparti actuellement à hauteur d'environ 80 % d'IT et 20 % d'OT.

La frontière n'est pas étanche entre ces deux domaines d'autant plus que l'évolution des usages fait que la demande de remontée d'informations, de mesures est croissante. La nécessité de connecter des outils industriels qui étaient souvent déconnectés du réseau (filaire ou Wifi) se fait de plus en plus présente ouvrant ainsi mécaniquement une porte d'accès pour des malveillants.

Le besoin de continuité numérique et d'analyse de données a, par exemple, amené les hôpitaux à développer leurs réseaux en connectant de plus en plus de systèmes sur internet et en offrant des accès Wifi. Ces réseaux mal sécurisés ont fait l'objet de nombreuses attaques ces dernières années avec des demandes de rançons sous la menace de divulgation de dossiers confidentiels ou une paralysie des services et des soins critiques comme, par exemple les salles d'opération. Dans cet exemple, le vol de dossiers confidentiels peut être rangé dans le domaine de l'IT alors que la prise de contrôle d'une salle d'opération le sera dans celui de l'OT.

Autre exemple moins médiatisé mais tout aussi problématique. Celui d'une station traitement des eaux dont les opérateurs ont perdu le contrôle de vanne sous l'effet d'une cyberattaque, menaçant ainsi de contaminer des circuits d'eaux potables. On comprend bien que de telles actions, sans être nécessairement d'une grande complexité, peuvent entraîner des conséquences délétères sur la santé des personnes et l'intégrité des matériels.

Alors, comment distinguer l'IT de l'OT ? Comme nous l'avons écrit, la frontière est poreuse mais l'OT comporte tout de même deux contraintes spécifiques :

- Les contraintes liées aux process. Nombreux process industriels nécessitent un fonctionnement en continu avec des exigences élevés en temps de réponse. Il est alors plus difficile d'intervenir et d'implémenter une solution cyber, et de la maintenir à jour …
- L'hétérogénéité des équipements : les systèmes industriels comportent de nombreux systèmes, capteurs, ordinateurs, automates … dont les caractéristiques sont très

hétérogènes. Les intervenants doivent posséder une solide culture industrielle pour y implémenter des solutions cyber.

Eiffage Energie Systèmes propose ses services de cybersécurité (majoritairement OT) dans l'industrie, les infrastructures et réseaux, le tertiaire et les villes et collectivités. Ils proposent de sécuriser les composantes de systèmes complexes (Serveur, postes utilisateurs, réseaux, automates, logiciels …) (figure 2).

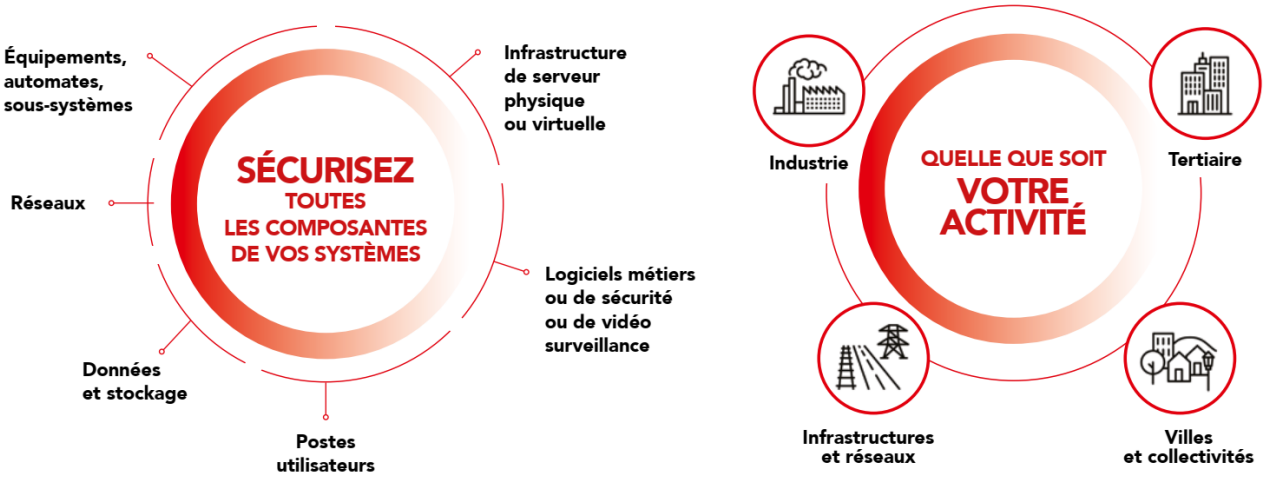


Figure 2 : Les domaines de la cybersécurité OT chez Eiffage

3 - Une prise de conscience d'un besoin à grande échelle

Ces menaces sont largement prises au sérieux par les autorités qui ont chargé l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) d'un rôle de communication et de préconisation auprès des opérateurs et des industriels.

On peut lire sur son site que « L'ANSSI, autorité nationale de cybersécurité, propose au premier ministre les mesures destinées à répondre aux crises affectant la sécurité des systèmes d'information des autorités publiques et des opérateurs régulés. Elle coordonne l'action gouvernementale et anime l'écosystème national. »

L'ANSSI a donc pour interlocuteurs des entreprises qui sont classées en fonction de leur importance lors de crises de cybersécurité. Ce sont des :

- Opérateurs d'Importance Vitale (OIV) : environ 200 organisations ayant des activités indispensables à la survie de la nation ou dangereuses pour la population [Wikipédia]. C'est le cas, par exemple, des gestionnaires d'installations nucléaires ou d'alimentation en eau, des acteurs du secteur militaire, ou des organismes opérant dans le domaine de la santé. Ces OIV sont tenus de développer des stratégies de cybersécurité pour protéger leurs activités.
- Opérateurs de Services Essentiels (OSE) : environ 1000 « opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services » (Article 5 de la loi du 26 février 2018.) Pour être considéré comme un OSE, l'entreprise doit répondre à trois critères :
    - Fournir au moins un service essentiel à la continuité d'activités économiques ou sociétales critiques ;

- Être tributaire des réseaux et des systèmes d'information pour la fourniture de ce service ;
- Être confronté à un risque de suspension de ce service en cas de cyber-incident.

Afin que ces OIV et OSE atteignent leurs objectifs l'ANSI édite en particulier :

- Des recommandations ;
- Un référentiel PIMSEC pour l'intégrateur (PAX pour le Neuf, PAMS pour la maintenance) ;
- Une méthode de gestion des risques EBIOS.

Les entreprises comme Eiffage Energie Systèmes qui proposent leurs services peuvent obtenir des qualifications pour les audits, la détection d'incident ou encore l'intervention après incident.

En complément des actions de l'ANSSI on peut noter que certaines collectivités territoriales sont pro actives dans ce domaine. Ainsi, la région Grand-Est propose une aide aux entreprises en prenant en charge 50% du coût d'un diagnostic de cybersécurité.

4 - Quelques « Success Stories »

Les projets réalisés par Eiffage Energie Systèmes sont très variés et basés sur trois types de prestations :

- **Audit, diagnostic et conseils :** il s'agit d'inventorier, d'évaluer les risques, de proposer un plan d'action pour atteindre un niveau de sécurité homologué.
- **Maintien en conditions de sécurité :** la veille de vulnérabilité et détection/qualification de nouvelles menaces, la formation de sensibilisation, l'amélioration continue, la simulation d'attaques et la réponse sur incident permettent de maintenir le niveau de sécurité à un niveau acceptable.
- **Sécurisation des systèmes :** l'intégration de solutions matérielles et logicielles (détection et protection), la remédiation et l'évaluation des risques résiduels permet de protéger les systèmes des risques de cyberattaque.

Á titre d'exemple de sécurisation, on peut citer :

- La sécurisation du contrôle-commande d'une ventilation nucléaire qui a nécessité la prise en compte de 3 000 entrées sorties physiques, 400 synoptiques.
- La sécurisation du contrôle-commande d'unité de contrôle des opérations sur le banc d'essai des accélérateurs à poudre situé à Kourou en Guyane française.
- La rénovation du système de vidéo-surveillance d'un site militaire par l'étude des risques de sécurité (cyberattaques, intrusions, piratages…) à l'aide de la méthode EBIOS.
- La rénovation du système de contrôle-commande d'une centrale électrique munie de groupes thermiques Diesel.
- La sécurisation de l'application TETRA de communication opérationnelle interne aux agents de la RATP.

Figure 3 : Visuel cybersécurité de Eiffage Energie Systèmes

La méthode suivie lors de ces projets commence par du « bon sens » : par exemple pour la sécurisation d'un automate, il faut renforcer les mots de passe, fermer les ports inutilisés, utiliser un VPN, segmenter l'architecture, ajouter des sondes …. Au-delà de ces premières mesures, il s'agit principalement d'un travail d'intégration basé sur la Norme de sécurisation de l'OT (ISO 62443).

Pour certains projets, il est nécessaire de réaliser des développements sur mesure. Ainsi dans le cas d'un système de supervision de contrôle commande avec des contraintes temps réel trop élevées, il a été nécessaire de développer un logiciel ad hoc.

5 - Et demain …

Chez Eiffage Energie Systèmes, on estime que le secteur de la cybersécurité OT est en pleine croissance et qu'il va falloir de nombreuses années pour mettre au niveau les systèmes industriels.

En effet, les menaces cyber ne font que croitre et les autorités souhaitent rehausser les niveaux de protection. Dans ce cadre, la directive NIS-2 (Directive Network and Information System Security 2) prévue pour le mois octobre 2024, aura pour conséquence de multiplier par 30 à 40 le nombre d'entreprises qui seront obligées de se cyber-sécuriser.

Ainsi, alors qu'aujourd'hui, Eiffage Energie Systèmes dispose de compétences Cyber dans quelques entités opérationnelles, il paraît fort probable qu'il faudra à terme des équipes cyber réparties sur tout le territoire au plus près des utilisateurs. Le potentiel d'emploi dans ce domaine est donc prometteur.

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay

Wattsense - Siemens, une entreprise pour une GTB sécurisée

La Revue 3EI
Culture Sciences de l'Ingénieur

Édité le 15/02/2024

école normale supérieure paris-saclay

Mohamed ZENADI[1] - Magali SAUVERGEAT[2]

[1] *Responsable Technique – Wattsense*
[2] *Enseignante BTS CIEL Arpajon*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

Cette ressource issue d'un entretien avec Mohamed Zenadi de la société Wattsense, présente la prise en compte de la cybersécurité pour les objets connectés par l'entreprise Wattsense. On y retrouve les concepts de cybersécurité réseaux décrits dans la ressource « Fondamentaux de la sécurité réseau » [5].

1 - L'historique de Wattsense

Wattsense est une start-up lyonnaise, elle est située à Dardilly, à proximité de Lyon, elle a démarré son activité en 2017. En octobre 2021, elle est acquise par Siemens et devient une unité autonome au sein de la division Siemens Smart Infrastructure. Les solutions développées par Wattsense permettent aux entreprises implantées dans l'Union européenne de se conformer à la directive sur la performance énergétique des bâtiments (DPEB).[1] [2]

Logo Wattsense - Siemens

Cette directive prévoit l'installation de systèmes d'automatisation et de contrôle des bâtiments dans le secteur tertiaire afin d'améliorer leur efficacité énergétique et de réduire leurs émissions de CO2.

2 - L'équipement : Wattsense Tower

Wattsense Tower est conçue pour connecter tous les types d'équipements de tous les bâtiments : capteurs IoT LoRa, compteurs, matériels de chauffage, de climatisation ou de traitement d'air, systèmes de gestion technique du bâtiment (GTB). Cet équipement s'interface également avec des équipements communicants et des consoles de supervisions via les protocoles M-Bus, KNX, Modbus, BACnet. [3]

Wattsense Tower se connecte automatiquement au cloud Wattsense via la 3G/4G, uniquement avec un port sortant (réduction de la surface vulnérable). Les données sont transférées régulièrement sur le cloud Wattsense, via un protocole sécurisé utilisant le protocole TLS qui assure authentification, confidentialité et intégrité. [4] Wattsense est autorité de certification pour délivrer les certificats TLS aux équipements.

Pour garantir la continuité de la sécurité, Wattsense Tower peut assurer la mise à jour de son firmware automatiquement via le réseau (mise à jour OTA Over the Air). Les firmwares téléchargés sont authentifiés via des certificats et leur intégrité est vérifiée.

Les données, stockées sur des bases de données dans des clouds privés virtuels (VPC) avec des pare-feux dédiés, peuvent être consultées via des pages Web sécurisées (HTTPS), permettant ainsi au client de configurer un ou plusieurs tableaux de bord (DashBoard). Le client a la liberté de sélectionner les données à afficher, de générer des graphiques, et même de définir des seuils d'alerte selon ses préférences.

Les connecteurs Webhook et MQTT offrent également la possibilité aux clients de recevoir le flux de données en temps-réel dans leurs infrastructures cloud d'entreprise, leur permettant ainsi de gérer ces flux. Parmi les plateformes possibles, on peut citer IoT Hub, IoT Core, Node-RED, et bien d'autres encore.

Le client peut également consulter à distance ces données via une API REST pour peupler une base de données interne, ou réaliser des applications internes de visualisation.

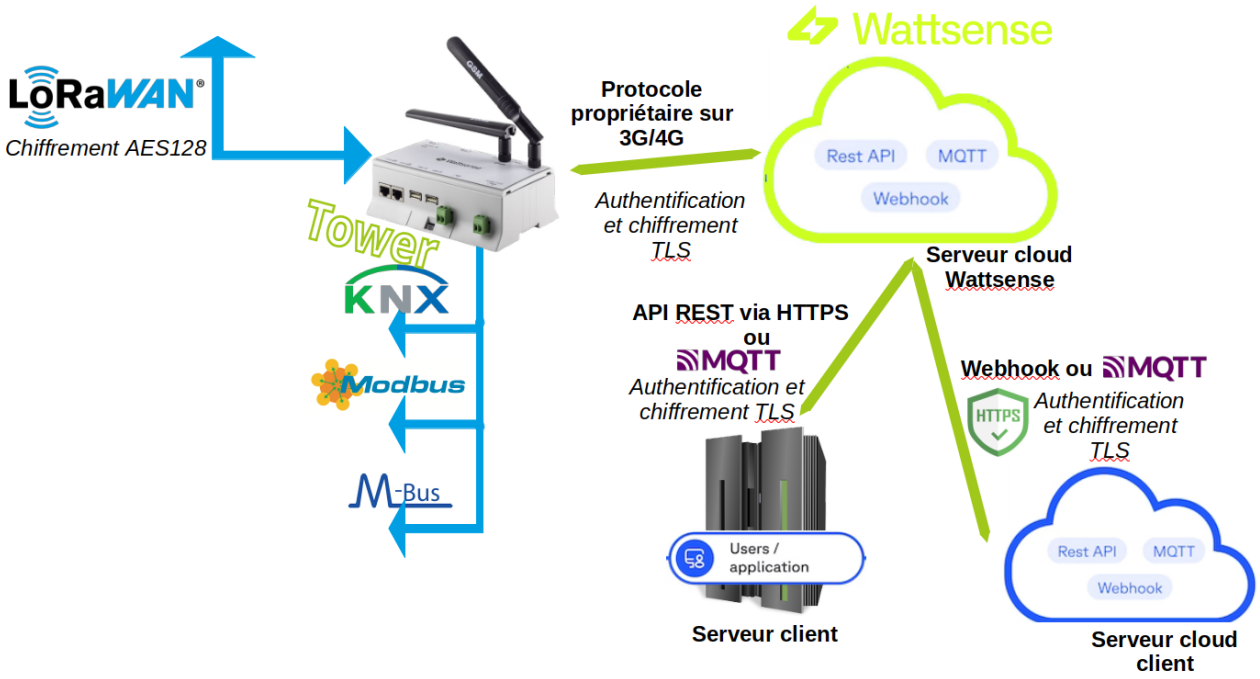


Schéma de l'architecture : Wattsense Tower

3 - Entretien avec Mohamed Zenadi, Wattsense

3EI : Pourquoi les trames LoRa sont déchiffrées dans l'équipement Tower et non sur le Cloud comme le prévoit l'architecture LoRaWan ?

Wattsense : Wattsense Tower s'intègre dans les architectures de supervision de nos clients avec par exemple le protocole Mbus. Afin de permettre l'intégration des équipements LoRaWan au sein de cette infrastructure locale, le décodage des trames doit être effectué au niveau de l'équipement Tower. Les données sont ensuite envoyées sur le cloud Wattsense en 3G/4G via le protocole sécurisé TLS.

3EI : Comment sont stockées les données sur le cloud Wattsense ?

Wattsense : Les données récoltées sont une première fois sauvegardées sous forme de données brutes puis sur une base de données MongoDB Time Series et redondées sur un deuxième cloud distant.

3EI : L'équipement Tower supporte le protocole LoRaWan v1.0, pourquoi le protocole LoRaWan v1.1 n'est-il pas supporté ?

Wattsense : La version 1.1 sera supportée dans la prochaine version de Tower. Cependant nos clients ne la demandent pas, car sur le marché de la GTB, il y a très peu d'équipements qui communiquent en LoRaWan v1.1.

3EI : Quels sont les fabricants d'équipements conseillés pour s'interfacer avec Wattsense Tower ? Exemple : (ADEUNIS, ATIM, ENLESS ...)

Wattsense : Wattsense Tower supporte 64 fabricants, il m'est difficile de privilégier un fabriquant plutôt qu'un autre. Je comprends que vous citiez ADEUNIS, ATIM, ENLESS car ce sont des fabricants français qui produisent des équipements de qualité, mais nous ne pouvons pas faire de recommandations pour un fabriquant plutôt qu'un autre.

3EI : MQTT et Webhook , quels sont les utilisations pour les entreprises ?

Wattsense : Lorsque le client souhaite récupérer le flux de données sans réaliser de développement interne, les webhooks, par leur facilité d'intégration, sont une solution performante qui permet au client d'automatiser des tâches et de déclencher des actions en temps réel.

MQTT est plus adapté aux communications bidirectionnelles, à la messagerie asynchrone et aux systèmes de messagerie plus complexes. Par rapport à MQTT, les Webhooks sont généralement plus simples à mettre en œuvre et sont souvent utilisés pour des communications unidirectionnelles en temps réel.

L'API REST est disponible pour les entreprises souhaitant réaliser un développement spécifique et récupérer les données archivées en interrogeant en différé le cloud Wattsense.

Références

[1] : Article *lyon-entreprises*
https://www.lyon-entreprises.com/actualites/article/internet-des-objets-la-start-up-lyonnaise-wattsense-rachetee-par-le-geant-allemand-siemens

[2] : DPEB : Performance énergétique des bâtiments
https://www.europarl.europa.eu/news/fr/press-room/20230206IPR72112/performance-energetique-des-batiments-neutralite-climatique-d-ici-2050

[3] : Le site Web de Wattsense
https://www.wattsense.com/

[4] : Wattsense : Sécurité IoT
https://www.wattsense.com/fr-fr/resources/securite-iot/

[5]: Fondamentaux de la sécurité réseau, M. Sechehaye, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/fondamentaux-dela-securite-reseau