COMPTE-RENDU
ATELIER OBJETS CONNECTES ET CYBERSECURITE

Animateur

Alain ESTABLIER, *Rédacteur en chef*
Security Defense Business Review

Participants

Maître François COUPEZ
ATIPIC Avocat

Antoine COUTANT, *Amossys*
Pôle d'excellence Cyber

Jean-Christophe DOUCEMENT
CESIN

Colonel Franck MARESCAL
OCSTI, PJGN

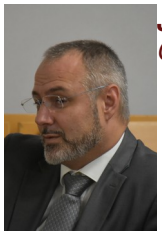
François STEPHAN
Institut de Recherche Technologique SystemX

Colonel Franck MARESCAL
OCSTI, PJGN

La sécurité liée aux véhicules est problématique : les voitures connectées sont enclines au piratage de données sensibles et au piratage système pouvant provoquer des accidents.
Exemple de Tesla et de ses véhicules autonomes qui ont eu droit à leur lot d'accidents (dérapages non contrôlés, etc.) malgré de multiples corrections et mises à jour du logiciel : Tesla en est à la 8ème version de son logiciel, c'est-à-dire qu'il y a eu 7 versions précédentes, il y a donc une avancée rapide pour corriger les failles en termes de cybersécurité mais l'avancée technologique est peut-être trop rapide.

« Les objets connectés sont en pleine prolifération : on en compte environ 6 milliards aujourd'hui et il y en aura bientôt 20 milliards. »

Aujourd'hui, les constructeurs sont à la recherche de la commercialisation de véhicules totalement autonomes : Renault et Valéo font actuellement de nombreux tests dans cette optique, et ils atteindront leur but d'ici une dizaine d'années selon le colonel Marescal.



Jean-Christophe DOUCEMENT
CESIN

Les objets connectés sont en pleine prolifération : on en compte environ 6 milliards aujourd'hui et il y en aura bientôt 20 milliards. Il existe une crainte liée à cette prolifération, car si on coupe les flux Internet, on a du mal à exister. De plus, si on est la cible de ce genre d'attaque : qu'est-ce qui masque une telle attaque ? Quel est le but ? N'y-a-t-il pas un but caché ?
Exemple des réfrigérateurs intelligents, thermostats électroniques, etc. qui peuvent être détournés : les gens ne pensent pas à les mettre à jour, et même les constructeurs ne font pas l'effort de les mettre à jour. Or il faut mettre à jour les softwares de manière régulière, ce qui n'est pas le cas aujourd'hui.

Usage des objets connectés dans le milieu bancaire : la banque est de plus en plus dématérialisée, mais certains clients viennent tout de même demander conseil auprès de leurs conseillers bancaires, et veulent garder ce lien. Ainsi, de plus en plus de personnes pensent aux lunettes à verres connectés, permettant aux deux interlocuteurs de parler directement et échanger intelligemment via verres connectés.

Question de la sécurité pour les verres connectés : si on se fait voler les lunettes, qu'est-ce qu'il reste ? Les données ont-elles été sécurisées et sauvegardées ? De plus, est-ce dangereux pour la banque ? Des lunettes qui peuvent prendre des photos des collaborateurs, des choses qu'il y a sur l'ordinateur du banquier etc. Le risque est réel pour la banque.

« C'est un marché jeune donc mal géré, mal régulé, la sécurité n'est pas forcément un critère de choix, même pour les constructeurs. »

Quels sont les risques relatifs aux vêtements connectés ? S'agissant des caméras connectés, la question se pose de savoir si nous sommes les seuls à avoir accès aux données. La réponse n'est pas évidente, car si nous y avons facilement accès, d'autres peuvent y accéder relativement simplement. Les mêmes questions se posent pour les bracelets connectés, les serrures connectées, etc. qui peuvent être détournés et souvent facilement.

Si une entreprise soupçonne un stagiaire de la voler ou de l'espionner, elle doit contacter la plus vite possible la DGSI. Intervention d'Alain Establier : "Avant, les étudiants étrangers, souvent asiatiques, rentraient dans les entreprises, les écoles, ou des enceintes tenues secret-défense, et prenaient des photos avec leurs lunettes connectées ; maintenant ils peuvent les envoyer en live directement à leurs pays."

« La question se pose de savoir si nous sommes les seuls à avoir accès aux données. La réponse n'est pas évidente, car si nous y avons facilement accès, d'autres peuvent y accéder relativement simplement. »

Antoine COUTANT, *Amossys*
Pôle d'excellence Cyber

Les logiciels de cryptographie "exotiques" sont moins efficaces que les logiciels de cryptographie français.
Il a fait le test de pirater des serrures électroniques achetées dans le commerce dont se servent des hôtels par exemple, et il a réalisé qu'il n'y avait aucun système de cryptographie pour sécuriser la serrure. Il existe donc de grosses failles en terme de sécurité.

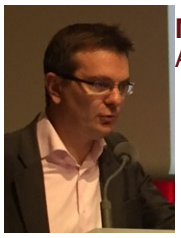
François STEPHAN
Institut de Recherche Technologique SystemX

SystemX est un bras armé de l'ANSSI dans la cybersécurité, l'ingénierie numérique des systèmes complexes : fabrication additive dans un laboratoire

de Safran par exemple, véhicules autonomes, territoires intelligents, etc. SystemX a un appui fort de l'ANSSI, il y a un fort levier de l'industrie française sur le volet sécurité numérique pour en faire un avantage compétitif en partageant les menaces.
SystemX et l'ANSSI font travailler ensemble en physique (aspect physique important pour le travail en synergie) des scientifiques, des chercheurs internes, des étudiants, des petites et grandes industries sur le plateau de Saclay (pôle d'excellence) pour créer une synergie.

« Il y a un fort levier de l'industrie française sur le volet sécurité numérique pour en faire un avantage compétitif en partageant les menaces. »

Par ailleurs, EDF s'est aussi installé sur le plateau de Saclay et travaille depuis avec SystemX sur les questions liées à la cybersécurité.
« 2016 est l'année du changement pour l'IoT et pour la cybersécurité » ;
« La cybersécurité est un enjeu de système, il faut avoir une approche système » ;
« Quand on parle d'IoT, on ne parle pas d'objets, on parle d'Internet of things, on en a fait une mauvaise traduction. »



Maître François COUPEZ
ATIPIC Avocat

On parle de plus en plus d'objets connectés en entreprise avec le concept de "BYOD" (Bring Your Own Device), ainsi les salariés viennent avec leurs propres objets connectés.

En reprenant l'exemple du stagiaire. L'employeur, par crainte qu'un stagiaire fasse une mauvaise utilisation des objets connectés va vouloir brouiller le signal du stagiaire. Cependant, est-il en droit de le faire ? La loi l'interdit, la peine encourue est de 6 mois d'emprisonnement et 35.000 euros d'amende (x 5 si c'est une entreprise).

Si les objets connectés sont piratés, que risquent les pirates ?
L'article 323-3 du Code Pénal interdit l'interception frauduleuse de données. Mais les peines encourues peuvent-être revues à la baisse comme ce fut le cas par la Cour de cassation qui a revu toute sa jurisprudence dans l'affaire Kerviel : l'amende est passée de 4,6 milliards à 1 million d'euros.

« L'article 323-3 du Code Pénal interdit l'interception frauduleuse de données. Mais les peines encourues peuvent-être revues à la baisse. »

Ainsi, le droit nous protège-t-il vraiment efficacement des failles en termes de sécurité ? Selon la CNIL, s'il y a des failles dans un logiciel, c'est à cause du développeur et c'est 150.000 euros d'amende, car dans les audits des entreprises on voit toutes les failles et c'est à l'entreprise de corriger les failles dès leur détection.

Colonel Franck MARESCAL
OCSTI, PJGN

Deux Secrétaires américains ont tenté de faire passer une loi pour obliger les constructeurs à intégrer de la sécurité dans les produits qu'ils vendent, car aucun des constructeurs n'a été capable de répondre en terme de sécurité. Des guides de bonnes pratiques commencent à paraître aux États-unis (comme le NIST Special Publication 800-160).

« On parle souvent de données à caractère personnel mais on en donne rarement la définition : ce sont toutes les données qui permettent de caractériser directement ou indirectement une personne. »

En Europe, l'équivalent de l'ANSSI européenne va sortir un guide prochainement, plus complet que les autres et plus détaillé, sur lequel 25 experts européens travaillent actuelement.
L'idée est la suivante : "Quand un constructeur met un produit sur le marché, il doit s'assurer d'un bon niveau de sécurité".

« « Privacy by design », c'est l'idée qu'il faut, dès la conception, s'assurer qu'on a produit toutes les diligences nécessaires pour la protection des données. »

Jean-Christophe DOUCEMENT
CESIN

« On parle souvent de données à caractère personnel mais on en donne rarement la définition : ce sont toutes les données qui permettent de caractériser directement ou indirectement une personne. »

Si on fait quoi que ce soit sur des données à caractère personnel, on est responsable vis-à-vis de la loi informatique et liberté.
Notion de « Privacy by design » aux États-Unis : protection dès la conception : dès la conception, on doit s'assurer qu'on a produit toutes les diligences nécessaires pour la protection des données.

« La Loi pour une République Numérique de 2016 prévoit une sanction de 3 millions d'euros au lieu de 150.000 euros auparavant en cas de manquement à la CNIL. »

À compter du 25 mai 2018, le Règlement Général sur la Protection de Données (RGPD) s'appliquera. Les sanctions en cas de manquement seront les suivantes :

20.000.000 d'euros ;

4% du chiffre d'affaires mondial consolidé pour le groupe (et non pas le CA d'une filiale. Par exemple, si la Banque Postale ne s'assure pas de la protection de données, c'est le groupe La Poste qui est sanctionné. Or le CA du groupe s'élève à 23 milliards d'euros, bien plus que la Banque postale. Les 4% s'appliqueront ainsi aux 23 milliards d'euros).

« Le Règlement Général sur la Protection de Données (RGPD) impose de ne travailler avec des sous-traitants que s'ils respectent le RGPD, c'est le premier critère. »

Maître François COUPEZ
ATIPIC Avocat

Ce sont les États-Unis qui sont surtout visés par ce texte : s'ils traitent des données européennes, la réglementation européenne va s'appliquer (extra-territorialité du droit de l'Union).

La Loi pour une République Numérique de 2016 prévoit une sanction de 3 millions d'euros au lieu de 150.000 euros auparavant en cas de manquement à la CNIL. De plus, on doit notifier les personnes dont les données ont été « violées » et notifier qu'on a été sanctionné. Elle prévoit aussi que les sous-traitants sont co-responsables et doivent ainsi respecter la RGPD.
L'article 28 impose de ne travailler avec des sous-traitants que s'ils respectent le RGPD, c'est le premier critère. En cas de non-respect, des sanctions en pourçentage du CA s'appliqueront.

La loi de modernisation de la justice du XXIe siècle de novembre 2016 prévoit l'action de groupe sur les données à caractère personnel. Qui peut agir ? Les associations de consommateurs, associations spécialement formées pour la protection des données à caractère personnel, les syndicats représentatifs. Mais n'est pas utile pour la partie sous-traitant d'ici le 25 mai 2018, avant que le RGPD ne soit appliqué.

Antoine COUTANT, Amossys
Pôle d'excellence Cyber

La donnée personnelle, qui permet de caractériser directement ou indirectement une personne, possède une valeur intrinsèque. C'est par le développement de la « Défense en profondeur » que l'on va pouvoir retarder un maximum les attaques (image des crocodiles et du pont-levis d'un château pour retarder l'attaque d'un ennemi).

« C'est par le développement de la « Défense en profondeur » que l'on va pouvoir retarder un maximum les attaques. »

François STEPHAN
Institut de Recherche Technologique
SystemX

On prévoit des attaques plus complexes encore, pour le moment on a une visualisation de la menace encore extrêmement basique, il y a beaucoup de recherches à faire pour développer la dataviz (datavizualisation) ainsi que la simulation pour pouvoir mieux simuler les risques pour tenter de faire des simulations qui collent aux risques réels.

Aujourd'hui les entreprises ne valorisent pas leur patrimoine immatériel, or l'information est le nerf de la guerre économique.

CE QU'IL FAUT RETENIR

⧫ Les objets connectés sont en pleine prolifération : on en compte environ 6 milliards aujourd'hui et il y en aura bientôt 20 milliards.

⧫ La question se pose de savoir si nous sommes les seuls à avoir accès aux données. La réponse n'est pas évidente, car si nous y avons facilement accès, d'autres peuvent y accéder relativement simplement.

⧫ On parle souvent de données à caractère personnel mais on en donne rarement la définition : ce sont toutes les données qui permettent de caractériser directement ou indirectement une personne.

⧫ « Privacy by design », c'est l'idée qu'il faut, dès la conception, s'assurer qu'on a produit toutes les diligences nécessaires pour la protection des données.

⧫ C'est par le développement de la « Défense en profondeur » que l'on va pouvoir retarder un maximum les attaques.