Lettre des "Lundi de la cybersécurité" no 53

Les attaques par canaux cachés

Cette menace insidieuse qui plane sur la confidentialité de vos données sensibles

Si je cause dans une conversation en surveillant alentours que personne d'autre que mon interlocuteur puisse entendre ce que je dis, mais qu'à grande distance, bien cachés, avec des jumelles, vous zoomez sur moi, au mouvement de mes lèvres, à l'éclat de mes yeux, aux plissements de mes paupières, aux gestes de mes mains, vous pourriez déduire, sans pouvoir m'écouter puisque vous êtes trop loin, des brides de ce que je suis en train de raconter. Dans cette conversation, je peux révéler un secret, sachant que je ne le ferais pas bien sûr si je pensais qu'une oreille indiscrète m'écoutait. Pas facile, certes mais avec le bon équipement, c'est envisageable. La conversation se déroule normalement, vous n'interceptez pas le son de ma voix, vous n'avez pas d'interférence avec ce que je dis, mais vous interprétez juste des signaux auxiliaires, à mon insu. Ils peuvent révéler mon secret... :-(

Dans le numérique, parmi toutes les technologies qui menacent vos informations, une catégorie peu connue mais dangereuse pour la confidentialité des informations que l'on utilise, que l'on stocke ou que l'on transmet est l'attaque basée sur les propriétés d'un équipement de chiffrement.

Un calculateur qui déroule un algorithme cryptographique consomme du courant électrique, avec des pics et des creux qu'un oscilloscope révèle. Cela induit des vulnérabilités qui peuvent renseigner sur les clés de chiffrement. La confidentialité des données est alors remise en question par ces dispositifs de cryptanalyse.

Et il n'y a pas que la consommation électrique… Les signaux électromagnétiques se propagent et sont donc enregistrables et identifiables. Les changements de tension au sein d'une résistance ou d'un condensateur s'accompagnent de vibrations mécaniques. L'activité électromagnétique, le bruit, le temps d'exécution d'un ordinateur qui opère une activité de chiffrement peuvent renseigner sur les clés de chiffrement utilisées. Ce travail de cryptanalyse n'est évidemment pas à la portée de tous, mais il y a des cryptanalystes qui sont redoutables pour interpréter ces signaux cachés.

Les câbles sous-marins qui acheminent la presque totalité des informations de l'Internet entre les continents, induisent moins de bruit que les explosions sur les pipelines de Nord Stream, mais peuvent être une source inépuisable de captation de secrets, surtout par des sous-marins équipés pour cette fonction.

Alors que faire quand on utilise des données sensibles ? Renoncer à sa liberté de circuler en s'enfermant dans une cage de Faraday, ainsi que le recommande la norme Tempest ? Blinder son smartphone en l'enfermant dans un boitier qui va décupler son poids pour en limiter le rayonnement électromagnétique ? Mon smartphone si léger dans un lourd boîter métallique, quelle horreur !

Il est sûr qu'il est utile de connaître ce que sont les attaques par canaux cachés, dites aussi attaques par canaux auxiliaires. Elles méritaient un Lundi de la cybersécurité ! C'est pour le Lundi de novembre, avec un de plus grands experts du domaine, le professeur Jean-Jacques Quisquater pour nous en parler.

Je donne la plume à l'intervenant

Merci à Gérard pour cette introduction qui contient déjà beaucoup d'éléments que nous expliquerons et détaillerons.

Ces attaques sont bien connues des militaires depuis longtemps et ce fut alors classifié. On parlait d'émissions compromettantes. Dans les années 80, elles furent pratiquement découvertes dans plusieurs laboratoires industriels en Europe sans être publiées et, je suis témoin, même censurées sans aucune action. Puis, en 1996, Paul Kocher publia sa première attaque en mesurant le temps d'exécution de divers algorithmes cryptographiques, à distance !, et il nous montrait qu'on pouvait ainsi récupérer la clé secrète. Ce fut alors le début d'une révolution, qui continue.

Nous parlerons en termes pratiques et illustrés de ces différentes attaques :

- les attaques passives où on "écoute" seulement les fuites de ces canaux cachés (son, temps, ondes électromagnétiques, etc) d'ordinateurs, serveurs, microprocesseurs et ces attaques ne peuvent donc pas être détectées : dans certains cas cela peut se faire à grande distance (sur internet)
- les attaques actives avec diverses méthodes d'injection (lumière, chaleur, laser, faisceau de cyclotron, ondes électromagnétiques, utilisation des protocoles, etc) pour engendrer des fautes transitoires ou permanentes qui perturbent les résultats des calculs. Le but le plus souvent est de capter les informations indirectes qui donneront, après transformations et calculs, la clé secrète convoitée. Ici, il faudra avoir accès ou être proche de l'objet attaqué mais c'est bien sûr possible pour beaucoup d'objets dans la nature (carte à puce, IoT, etc).

Il existe de nombreuses contremesures à ces attaques, bien appliquées dans le domaine des cartes à puce. Dans le cas de la consommation électrique (attaques dites SPA et DPA), les contremesures ont été vigoureusement brevetées et ont donné lieu à une lutte juridique intense entre les inventeurs (ils furent les gagnants) et les principales firmes de carte à puce.

Plusieurs conférences internationales, CARDIS, CHES, et autres, reprennent ces recherches actuelles et sont fort suivies.

Les attaques les plus subtiles (Spectre, Meltdown), liées aux caches ou à la prédiction d'instructions, ont été contenues en imposant une nouvelle conception des processeurs à Intel, AMD, IBM, etc.

Ces attaques ne sont pas confinées au matériel mais bien aussi, et surtout dans les cas pratiques, au logiciel. Un logiciel qui utilise une clé secrète en un temps non constant est un logiciel dangereux et il y en a beaucoup. Un autre vecteur d'attaque est un programme espion qui parvient à partager un processeur avec un programme cible. L'imagination est donc bien au pouvoir.

Je reprends la plume

Qui est Jean-Jacques Quisquater ?

Jean-Jacques Quisquater, est un cryptologue belge, professeur à l'université catholique de Louvain en Belgique, et membre de l'ARCSI. Docteur d'État en science informatique obtenu au Laboratoire de recherche en informatique de l'université d'Orsay, il est membre de l'IEEE.

UCL Université catholique de Louvain

Académicien à l'Académie royale de Belgique, il figure parmi les pionniers de la blockchain et de la carte à puce. Il interviendra bien sûr aussi à la BNF aux 14èmes rencontres de l'ARCSI, voir ci-après.

Demande d'inscription pour le Lundi de la cybersécurité de novembre

lundi 14 novembre à partir de 18 h 00, en distanciel, par visio conférence Zoom et nous reprenons en parallèle les présentiels à Université Paris Cité (nouveau nom de l'université de Paris), 45 rue des Saints-Pères Paris 6e.

Nos « Lundi de la cybersécurité » **sont gratuits** et veulent vous offrir une fête technologique qui marque les esprits, nous nous y employons. **Demandez votre inscription, par courriel** et vous recevrez un hyperlien personnel vers la visioconférence un peu avant le jour de l'événement, et, quand c'est aussi en présentiel, les coordonnées de l'amphi.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans le message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

Et n'oubliez pas de préciser si vous souhaitez être en présentiel 45 rue de Saints-Pères Paris 6e ou à distance par Zoom.

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués à l'intervenant.

Un quart d'heure avec l'ANSSI

Avec Philippe LAVAULT, Chef des ressources extérieures de l'ANSSI

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant ou de l'intervenante et la session questions / réponses, autour de 19h15, nous donnons pour quinze minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'Information.

Après 20 ans passés au ministère des Armées, Philippe Lavault a rejoint l'ANSSI il y a 5 ans. Il est ainsi très bien placé pour nous parler de cet organisme, qui délivre des certifications sur les solutions de cybersécurité (Critères Communs, CSPN), pour nous évoquer les solutions comme SecNumEdu pour les formations, comme SecNumCloud pour l'hébergement dans les nuages. L'ANSSI peut intervenir pour aider les Opérateurs d'Importance Vitale (OIV), les Opérateurs de Services Essentiels (OSE), les ministères, à faire face aux cyberattaques, parmi les nombreuses missions de l'ANSSI.

Philippe Lavault est aussi co-auteur d'un thriller captivant, le protocole Magog. Sur fond de technologies cyber, de luttes d'influence géostratégiques et de relations de pouvoir, ce thriller met en scène le chaos qui pourrait résulter d'une perte de contrôle de nos données numériques et les moyens à notre disposition pour y faire face

Retour sur les Lundi de la cybersécurité précédents.

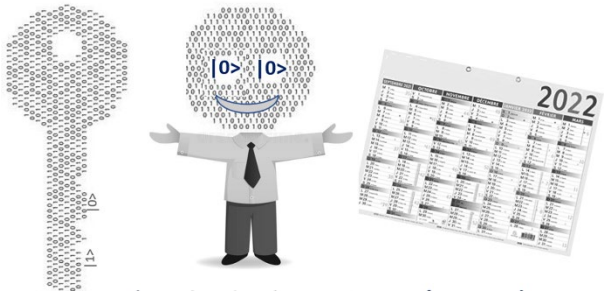
Vous trouverez tous les détails, slides, enregistrements sur le web de l'ARCSI, en https://www.arcsi.fr/ pour les plus récents et en https://www.arcsi.fr/evt_passes.php pour les évènements plus anciens. Les quarts d'heures accordés aux associations se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui se sont déjà exprimées dans nos Lundi précédents.

Vous avez aussi le détail et l'invitation de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information qui organise le jeudi 20 octobre, à la BNF (Bibliothèque Nationale de France) Paris 13e, les **14e rencontres de l'ARCSI** sur « ***l'épopée de la carte à puce et son avenir*** ». Pour cet évènement, les inscriptions sont encore ouvertes mais limitées en nombre par la taille de l'amphi.

Voir la plaquette en : https://www.arcsi.fr/doc/R14-Plaquette.pdf
Formulaire d'inscription en : https://www.arcsi.fr/inscription-R14/form.php

Merci à Francis Bruckmann, webmestre et membre du Conseil d'Administration de l'ARCSI pour tout son travail afin que la mémoire de nos « Lundi de la cybersécurité » ne soit pas perdue.

Gérard



Lundi de la cybersécurité de décembre 14 dec.

avec Bénédicte Pilliet

Présidente du Cybercercle