Vers de nouveaux concepts cryptographiques 1/2

Revue militaire générale n°54

le chef de bataillon Mathieu MORALES

publié le 21/03/2019

Sciences & technologies

Alors qu'une faille de sécurité nécessite souvent plusieurs années pour être comblée, l'interconnexion des systèmes poursuit sa progression exponentielle et ouvre la voie à de nouvelles menaces. Si, aujourd'hui, les puissances de calcul restent relativement limitées, les attaques massives aux conséquences de plus en plus importantes se multiplient et mettent en exergue les lacunes du système. En parallèle, l'avènement des ordinateurs quantiques dans les années proches viendra remettre en cause le fondement même de nos concepts de sécurisation des transmissions. Le chef de bataillon Morales considère que la recherche cryptographique revêt dès aujourd'hui un enjeu stratégique pour faire face aux menaces de demain.

Depuis sa banalisation dans les années 90, Internet n'a cessé d'évoluer pour s'adapter aux demandes et besoins des utilisateurs.

Ainsi, une part croissante des systèmes se retrouve connectée alors qu'elle n'était pas prévue de l'être. Les systèmes sont rarement réinventés, et le développement informatique moderne tend à ajouter des briques logicielles ou interfaces à des briques existantes. Des failles de sécurité existent depuis l'origine de l'informatique et perdurent sans qu'aucun composant n'y échappe. Parfois il faut de longues années pour y remédier. Dirty cow[50] a par exemple nécessité neuf ans pour être corrigée.

Plus récemment, c'est une faille découverte dans le protocole WPA2 (sécurisation des accès aux réseaux wifi) qui fait l'actualité. Au-delà de la faille elle-même, c'est le délai qui sera nécessaire pour l'abolir qui inquiète la commission nationale de l'informatique et des libertés (CNIL)[51].

Les menaces actuelles

En 2010, le vers STUXNET[52] avait surpris la communauté internationale car il la première cyber-arme reconnue. Ainsi, sans contact physique ni troupes déployées, les États-Unis étaient parvenus à stopper le programme nucléaire iranien en profitant des connexions nécessaires à la mise à jour des équipements nucléaires.

Mais ces techniques ne sont plus aujourd'hui l'apanage d'acteurs étatiques. 2017 a été le théâtre de plusieurs actions de grande envergure. Une des plus massives fut WannaCry qui toucha de nombreuses entreprises dans le monde entier. Ce ransomware exploitait la faille EternalBlue[53] des systèmes Windows antérieurs à Window10. Une fois en place, le virus chiffrait toutes les données qui ne pouvaient être déchiffrées qu'en payant une rançon. Windows XP, qui tourne encore dans de nombreuses entreprises (entre autres de nombreux distributeurs automatiques de billets), a été le plus touché et a permis la propagation du virus. Dans le même temps, Adylkuzz se basait sur la même faille pour utiliser les ordinateurs contaminés à produire de la crypto monnaie, les gains pour les pirates étant estimés à un million de dollars. Enfin, l'été dernier, NotPeya a touché de grandes entreprises en perturbant une partie de leur activité ; en France, le géant Saint-Gobain a vu certaines de ses filiales (Lapeyre, Point P) complétement paralysées. Le groupe a estimé à 220 millions d'euros sa perte en revenus sur les six premiers mois de l'année, soit 1,1 % de son chiffre d'affaires[54]. Ces attaques touchent non seulement les entreprises, mais aussi les infrastructures sensibles et stratégiques sans que les dégâts collatéraux ne puissent être contrôlés (hôpitaux, institutions étatiques et centrales nucléaires).

Notre société s'est ainsi progressivement laissé déborder par les multiples connexions de réseaux et peine à contrôler, d'une part la quantité et d'autre part le cheminement des informations circulant sur la toile. Pourtant, les technologies modernes autant que les recherches tendent à accentuer davantage la circulation et l'éparpillement des données.

Évolution des menaces

Le web 2.0 et l'invention des smartphones ont bouleversé les utilisations et les systèmes de valeurs. Nous sommes aujourd'hui aux prémices de ce que beaucoup considèrent comme la troisième révolution numérique avec l'apparition de l'« internet of things ». Au smartphone et autres montres connectées viennent désormais s'ajouter de nombreux autres objets du quotidien (ampoule programmable, volet contrôlable à distance, voiture connectée etc.). Ils constituent un maillage de plus en plus dense avec son lot de vulnérabilités car il n'existe pas encore de standard de sécurité appliqué à ces nouvelles technologies. Les vulnérabilités sont le plus souvent situées au niveau des micrologiciels permettant d'interagir avec le matériel (firmwares). Ces derniers sont difficiles à sécuriser car il n'existe pas d'antivirus et parce que chaque composant a ses propres spécificités. Dans un second temps, le non-respect des bonnes pratiques de sécurité est trop souvent observé (par exemple ne pas changer les identifiants par défaut) et amplifie les problématiques de sécurité.

Certes le commerce des objets connectés a commencé dans les domaines du loisir et de la domotique, mais c'est dans le médical que les progrès sont le plus attendus. Combinés avec les technologies big Data, des capteurs de données, embarqués sur les patients, pourraient permettre de prédire de façon statistique les risques de récidive d'une maladie grave ou encore alerter un médecin d'un incident. Afin que ces objets conservent une certaine ergonomie, les informations mesurées sont transmises vers des structures plus importantes qui les stockent et les traitent. Les quantités de données vont croissant et

nécessitent des puissances de calcul de plus en plus grandes.

Nos armées ne font pas exception. Depuis plusieurs années, la numérisation de l'espace de bataille est un enjeu considérable et les systèmes en interaction ne cessent de s'accroître. Qu'il s'agisse du combattant avec le système Félin, de communications avec des drones, ou de la robotisation, tous concourent à une multitude de transmissions de données.

Ainsi, alors que les interconnexions des systèmes sont d'ores et déjà sources de menaces, les vulnérabilités et portes dérobées pour accéder aux informations vont se multiplier et nécessiteront de nouveaux protocoles de sécurisation des échanges.

La sécurisation des informations

A l'heure actuelle, il existe deux types de chiffrement, l'un dit symétrique, l'autre dit asymétrique.

Dans le cas du chiffrement symétrique, une clé unique est utilisée à la fois pour chiffrer les données et les déchiffrer. Parmi les plus connus, on retiendra le « masque jetable » ou chiffrement de Vigenère, réputé inviolable en suivant des règles de génération de clés précises. Les plus couramment utilisés sont le triple DES et AES. Si ce type de chiffrement offre des niveaux de sécurité relativement satisfaisants, il pose des problèmes de transmission de clé.

Afin de pallier cela, Whitfield Diffie et Martin Hellman présentent au public le concept de chiffrement asymétrique à la National Computer Conference en 1976. Le chiffrement repose sur une paire de clés ; la première, rendue publique, sert à chiffrer les données ; l'autre, gardée secrète, sert à déchiffrer. Il n'est donc plus nécessaire d'échanger les clés. Les chiffrements à clés publiques sont très répandus sur internet et constituent la base de la quasi-totalité des transmissions sécurisées. Le plus connu est le RSA[55] utilisé dans les connexions SSL/TLS[56], les paiements en ligne, les signatures électroniques et les messageries sécurisées de type PGP[57].

Deux principes mathématiques entourent le concept de chiffrement asymétrique : le problème du logarithme discret et la décomposition en nombres premiers. Dans les deux cas, il n'existe pas d'algorithme efficace de résolution et il est nécessaire d'essayer toutes les combinaisons pour trouver celle qui donne le résultat escompté. Ainsi, bien qu'il soit possible de déchiffrer les messages sans la clé privée, cette opération nécessite des puissances de calcul non disponibles. Le principe est donc de jouer sur les temps de déchiffrage. Cette manipulation peut prendre plusieurs années avec des algorithmes classiques et l'informatique moderne, mais ces délais seront considérablement réduits avec l'avènement des calculateurs quantiques.

50 Faille permettant d'obtenir des privilèges sans laisser de traces sur le système Linux : http://www.zdnet.fr/actualites/dirty-cow-une-faille-vieille-de-9-ans-corrigee-au-sein- du-noyau-linux-39843818.htm

51 https://www.numerama.com/tech/298472-lanssi-salarme-la-faille-krack-va-nous-faire- vivre-pendant-des-annees-avec-des-wi-fi-perces.html

52 https://www.nouv

elobs.com/rue89/rue89-internet/20120604.RUE0433/stuxnet-comment-les-etats-unis-et-israel-ont-pirate-le-nucleaire-iranien.html

53 https://fr.wikipedia.org/wiki/EternalBlue

54 http://www.zdnet.fr/actualites/notpetya-a-coute-cher-a-saint-gobain-39855594.html

55 Le chiffrement RSA (nommé par les initiales de ses trois inventeurs) est un algorithme de cryptographie asymétrique très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman.

56 Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre deux machines communiquant sur Internet ou dans un réseau interne.

Titre : le chef de bataillon Mathieu MORALES

Auteur(s) : le chef de bataillon Mathieu MORALES

Date de parution 14/03/2019