Le chaos à la rescousse de la sécurité

La théorie du chaos a été découverte dans le domaine des mathématiques et a commencé à être observée dans la vie quotidienne au cours de la seconde moitié du vingtième siècle. Le chaos est une théorie scientifique qui vise à expliquer voire à donner une certaine prévisibilité à des systèmes complexes. À première vue, la théorie du chaos ressemble, comme la plupart des découvertes mathématiques, à une coquetterie de l'esprit. Par exemple, imaginez un chercheur qui passe ses journées à regarder le ciel pour trouver une certaine logique dans la dissipation des nuages ou un scientifique qui compte les branches d'un flocon de neige. On peut s'interroger sur l'importance d'un nuage dissipé ou sur l'acte de reproduire à l'infini un minuscule flocon de neige. Pourtant, en utilisant ces bizarreries (systèmes chaotiques), les mathématiciens ont trouvé des « patterns », c'est-à-dire des modèles mathématiques entièrement prévisibles, appelés attracteurs étranges. La théorie du chaos a également permis la découverte de dimensions de l'espace qui ne sont plus entières, appelées fractales. Par exemple, une ligne brisée formée de quatre segments de même longueur est considérée comme une ligne fractale de dimension un quart (¼). Revenons à ces répétitions à l'infini du même modèle. Elles se retrouvent partout dans des phénomènes naturels, par exemple les vaisseaux sanguins, les fleurs de brocoli ou les chaînes de montagnes. Les prévisions météorologiques utilisent la théorie du chaos tous les jours. Des processus chaotiques sont également utilisés en économie, pour améliorer la température ambiante dans une pièce, pour comprendre la turbulence dans l'aviation, pour expliquer l'augmentation du nombre de cellules cérébrales ou encore concevoir de nouvelles méthodes de chiffrement en technologie de l'information. Enfin, comme nous allons le démontrer, l'introduction de processus chaotiques dans la technologie peut aider à résoudre, de façon substantielle, les problèmes de sécurité informatique.

L'émergence du Chaos

En se basant sur l'observation de certains phénomènes, les physiciens ont abouti à deux conclusions paradoxales :

- Un certain degré d'uniformité et d'ordre peut être trouvé dans des phénomènes apparemment erratiques et incontrôlables.
- Un phénomène très contrôlable et prévisible, tel que la trajectoire d'une planète autour du soleil, peut devenir très imprévisible sur une période de plusieurs dizaines de millions d'années.

Jean Jacques Raphael, CISA, CISM, ISO 27001 LI
Est chargé de Cybersécurité à OCTOSAFES Inc. Il est un gold ISACA® member » au chapitre de Montréal (Québec, Canada).

Jean Claude Célestin
Est chargé de Travaux pratiques à l'Université d'Ottawa (Canada). Il est un ancien Administrateur de Réseaux.

Eric Romuald Djiethieu, FCNSP, ISO 27002 Foundation, ITIL
Est Architecte en télécommunication et en solutions de sécurité à Desjardins. Il est aussi un cofondateur de OCTOSAFES Inc.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Les concepts de la théorie du chaos mentionnés précédemment peuvent être utilisés pour trouver des solutions optimales aux problèmes de sécurité critiques des systèmes d'information, tels que le vol d'identité et la contrefaçon, et pour renforcer la sécurité des systèmes d'information. Ceci peut être illustré à travers l'exemple d'une nouvelle carte d'identification électronique. Cette carte intègre des processus chaotiques dans tous les aspects de son fonctionnement et de sa conception. Du câblage erratique des microcircuits, aux variations fréquentielles de communication en passant par les imperfections dans la structure physique du matériel.

Nos hypothèses de départ

Notre approche pour trouver des solutions de sécurité basées sur le chaos repose sur cinq hypothèses. Les deux dernières hypothèses sont déduites des trois premières :

- **Hypothèse 1 (H1)**—Un enfant, qui nait aujourd'hui, n'a besoin ni d'un nom ni d'un numéro pour être identifié et authentifié par une machine.
- **Hypothèse 2 (H2)**—À une certaine échelle (micromètre ou microseconde), il est impossible que deux personnes ou deux objets soient exactement identiques, par exemple des jumeaux, des empreintes digitales ou deux feuilles de papier issues d'une même rame.
- **Hypothèse 3 (H3)**—Pour devenir plus sûrs, voire inviolables, les systèmes d'information doivent obéir à de nouvelles lois et à une nouvelle logique (autre que la logique booléenne).
- **Hypothèse 4 (H4)**—La machine peut nous protéger en se protégeant.
- **Hypothèse 5 (H5)**—Il est maintenant possible, sur la base des hypothèses précédentes, de concevoir des systèmes d'information avec une compatibilité limitée (c'est-à-dire, il peut devenir impossible pour deux machines de communiquer sans une certaine interaction préalable).

Les deux dernières hypothèses sont déduites des trois premières:

La numérisation du chaos pour une nouvelle cybernétique

Bien des scientifiques et des technologues ont tenté par de nouvelles méthodes de modifier le fonctionnement des systèmes d'information, notamment en codant les informations de la même manière que l'ADN (quatre états initiaux) ou en y appliquant la théorie quantique (bits quantiques). La numérisation du chaos est, d'après nous un moyen encore plus adéquat pour résoudre, dans l'immédiat et en prévision de l'avenir, les problèmes de sécurité des systèmes d'information.

Notre démarche vise à protéger les données personnelles et les machines (ordinateurs, avions et drones, par exemple) contre toute manipulation accidentelle ou malveillante ou encore à garantir l'authenticité (des médicaments, du vin, des parfums, par exemple). Pour illustrer nos hypothèses, nous avons conçu une machine présentant des circuits logiques et fonctionnant à l'aide d'algorithmes chaotiques. Cette machine est une simple carte à puce en polymère ayant les dimensions d'une carte de crédit. Lorsqu'elle est utilisée pour protéger les renseignements personnels, cette carte stocke les données génétiques, biométriques et la date de naissance du nouveau-né. Cette carte fera partie intégrante de la vie de son titulaire (de la naissance à la mort) et l'aidera à s'identifier et s'authentifier lors de certaines activités cruciales où les critères de confidentialité, d'intégrité et de disponibilité doivent être strictement respectés.

Notre système informatique utilise la logique booléenne traditionnelle et le modèle OSI[1] (Open Systems Interconnection), mais ces outils sont utilisés à l'échelle sous-millimétrique et à des intervalles de temps de l'ordre de la microseconde. La sécurité étant, pour nous avant tout, une question de support, les caractéristiques physiques de notre carte seront mises à contribution pour garantir de bout en bout la légitimité de toute transaction. Chaque fois que la carte communique avec un serveur d'authentification (peu importe la distance), un contact physique est maintenu. Dès que ce contact est rompu, la communication est annulée.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Description de la carte à puce

La carte doit être fabriquée avec un polymère stable et inaltérable par la température ou le temps. Un revêtement en verre réfractaire la protège du feu.

Ce médium familier peut devenir un système complexe lorsqu'il est soumis à une analyse spatio-temporelle. À l'échelle humaine, Il est impossible de distinguer 2 cartes à l'aide de la vue et du toucher. Mais si ces 2 cartes sont balayées avec un faisceau laser de quelques microns de diamètre, des différences notables apparaissent (prouvant l'hypothèse H2). Ce balayage fait apparaitre ici et là des bosses et des creux. De plus, la machine qui insère la puce sur les cartes possède un certain degré de liberté lors du placement de ces puces. Par exemple, la puce de la carte 1 est placée à 10 microns du côté droit de la carte, la puce de la carte 2 est placée à 11 microns du côté droit de la carte et la puce de la carte 3 est placée à 12 microns du côté droit de la carte. Ces légères variations, indétectables à l'œil nu, renforcent le caractère unique de chaque carte.

La machine qui produit ces cartes peut renforcer encore leur unicité en enregistrant leur heure de création. Par exemple, si la carte 1 a été créée le 22 décembre 2018 à 2h: 35m: 00s: 01ms et la carte 2 a été créée le 22 décembre 2018 à 2h: 35m: 00s: 02ms, cette différence en millisecondes est une valeur clé pour renforcer une fois de plus, le caractère unique de chaque carte.

Ces variations dans la topologie et le temps de fabrication de chaque carte sont enregistrées sur le disque dur du serveur d'authentification (AS). Ces informations sont répliquées en moins de 24 heures sur d'autres serveurs répartis dans un rayon de plus de 100 km, assurant ainsi une sauvegarde. Si un titulaire perd sa carte, le processus reprend en fonction des informations contenues sur le serveur d'authentification et les données immuables du titulaire de carte (date de naissance, données génétiques et biométriques). Ces données sont transférées sur une nouvelle carte. Les informations figurant sur la carte perdue sont envoyées sur un autre serveur et conservées pendant une décennie. La carte perdue est définitivement inutilisable et détruite si elle réapparaît.

Les données génétiques et biométriques d'un nouveau-né sont enregistrées et analysées par le serveur d'authentification (AS) qui stocke les caractéristiques physiques de la carte, les données génétiques et biométriques de l'enfant et sa date de naissance à la milliseconde près. Cet AS reste la propriété du gouvernement et devra être reproduit dans certains bureaux du gouvernement, tels que les hôpitaux et les ambassades. La carte à puce communique avec cet AS chaque fois que l'identité de cet enfant doit être authentifiée. Les données biométriques (empreintes digitales) et génétiques (ADN) sont plus que suffisantes pour authentifier l'identité de l'enfant, prouvant ainsi l'hypothèse H1. Pour des raisons de responsabilité juridique, il convient d'ajouter les données génétiques et biométriques de la personne responsable de l'enfant (par exemple, un parent ou un tuteur). Un nom et un numéro de sécurité sociale (SSN) doivent être ajoutés à la carte, mais ces informations ne permettront pas à quelqu'un d'effectuer une transaction frauduleuse en se faisant passer pour cette personne. De plus, le nom et le numéro de sécurité sociale de la personne doivent être imprimés sur la carte, car c'est le seul moyen de distinguer les cartes lors de la collecte de données en masse.

Chaos et Cybersécurité

La théorie du chaos révèle, comme nous l'avons dit, deux réalités de la vie quotidienne :

- Il est possible de côtoyer l'infini à partir d'un espace limité et fini. Par exemple, l'analyse montre que, sous grossissement, un flocon de neige a toujours six branches et que sur chacune de ces branches, il y a six branches plus petites… et ainsi de suite. Plus le flocon est agrandi, plus on peut observer un plus grand nombre d'embranchements.
- Il est souvent impossible de prédire de manière déterministe ou aléatoire le résultat d'un système. Par exemple, il est impossible, sur la base de l'attraction d'autres planètes ou même de la lune, de prédire avec précision la position de la Terre par rapport au soleil après 10 millions d'années.

© 2019 ISACA. All rights reserved. *www.isaca.org*

Afin de démontrer l'intégration du chaos dans la cybersécurité, nous allons nous baser sur l'exemple qui suit : trois cartes sont la propriété de Jean, Claude et Éric. Ces trois cartes ont été initialisées par une interaction avec le serveur d'authentification décrit précédemment. À partir de cette phase, ces deux machines (la carte et le AS) peuvent décider de communiquer entre elles en utilisant uniquement des bandes de fréquences bien définies. Pour Jean, l'analyse de la surface de la carte et la transmission des données sont effectuées de manière aléatoire et non répétitive sur les bandes de fréquences suivantes : 0 à 10 GHz, 50 à 70 GHz et 200 à 205 GHz. Pour Claude, on utilise les bandes de 15 à 20 GHz, de 40 à 60 GHz et de 201 à 206 GHz ; pour Éric, les bandes de 7 à 9 GHz, de 80 à 90 GHz et de 205 à 305 GHz sont utilisées.

Ces variations de fréquence uniques et imprévisibles sont associées à d'autres informations chiffrées (voir la figure 1 comme exemple) : le montant qui sera retiré, le nom de la banque, le numéro de compte, l'heure, la latitude et la longitude du guichet automatique, les données biométriques et génétiques du client, les caractéristiques physiques de la carte associés à la fréquence permise uniquement pour cette transaction rendront inopérantes toutes tentatives d'utilisation frauduleuse.

Comme le flocon de neige dont le nombre de branches observables dépend du grossissement, la structure physique de chaque carte varie avec chaque variation de fréquence : Le nombre de creux (0) et de bosses (1) varie lorsque la fréquence de balayage est, par exemple, de 10 ou 2,5 GHz. Seul le système (serveur d'authentification et carte) peut savoir si la fréquence utilisée est permise (hypothèse H4 vérifiée). L'unicité de chaque transaction, associée à d'autres mécanismes de chiffrement, garantit l'inviolabilité du système.

Les données génétiques et biométriques étant collectées et analysées à l'échelle du micromètre, elles ne peuvent pas être reproduites (hypothèse H2). L'examen et le stockage de cette quantité phénoménale d'informations à ces échelles microscopiques sont possibles du fait que, de nos jours, des téraoctets de données sont sauvegardés dans des volumes de plus en plus petits.

Seule la machine peut identifier ces données ou les rejeter (hypothèse H4) lorsque quelqu'un tente de les reproduire. Tout écart par rapport à la configuration initiale (quelques microns ou microsecondes) provoque un rejet. Pour reproduire tous les détails du système, les capacités sensorielles d'une personne auraient besoin d'un amplification moyenne de l'ordre de 1 000 pour pouvoir détecter les infimes informations contenues sur une carte. En raison de la dimension temporelle, il sera quand même impossible de reproduire les mêmes données même en utilisant la même machine.

Un autre exemple illustre un cas limite : des enfants jumeaux présentant des caractéristiques génétiques et physiques assez similaires naissent le même jour. Étant donné que les enfants jumeaux ne naissent jamais au même moment (à la microseconde près), que leur biométrie est différente (au micromètre près) et que leurs actes de naissance sont imprimés sur des cartes séparées avec des caractéristiques microscopiques distinctes, il est impossible pour l'un de prétendre être l'autre. Le système peut différencier ces deux enfants car la communication entre l'AS et la carte peut révéler certains détails microscopiques qui différencient ces enfants. Par exemple, seules la carte et l'AS savent combien de microsecondes se sont écoulées entre l'impression des deux cartes, combien de creux distinguent la deuxième carte de la première et combien de micromètres différencient la paume de chaque enfant. Ces quantités microscopiques seront indétectables et inutiles pour les gens, mais les deux systèmes pourront les enregistrer fidèlement pour empêcher à un enfant de voler l'identité de l'autre.

S'attaquer aux faiblesses de la biométrie numérisée

L'une des faiblesses des systèmes de sécurité fondés sur la biométrie est que les données proviennent d'un échantillon numérisé (hypothèse H3). Le cas est différent pour le système proposé par nous. La machine détecte l'effet de relief (la

© 2019 ISACA. All rights reserved. *www.isaca.org*

rugosité de la surface) de la carte. En nous référant à la couche 1 du modèle OSI, les caractéristiques physiques du système (la carte et l'AS travaillant ensemble) ne se limitent pas à la circulation électronique ou à la bande passante. Le serveur d'authentification de la machine vérifie la rugosité initiale d'une carte pour s'assurer qu'il s'agit bien de la même carte qu'elle a analysée initialement et conservée en mémoire. Si l'AS ne trouve pas la même topographie, elle refuse d'authentifier la transaction. Étant donné que cette rugosité est numérisée (par exemple, 1 indique une bosse, 0 indique un creux), cette information fait partie du processus de chiffrement et peut même faire partie de la clé pour décoder l'information utile. Cette rugosité n'existe pas dans les systèmes actuels. La capacité de décodage assure l'inviolabilité du système. En effet, un « man in the middle » peut toujours avoir à sa disposition un compilateur classique ou quantique, il ne pourra jamais déterminer si tel bit isolé constitue une partie du support physique de l'information ou représente une partie de l'information elle-même.

Auto-protection et compatibilité limitée

Les hypothèses H4 et H5 concernent les protocoles de sécurité qui s'établissent entre le serveur d'authentification et la carte. Les systèmes formés par la carte et le serveur ne deviennent compatibles (hypothèse H5) qu'après une interaction initiale. Lors de ce premier contact, certains protocoles de communication sont établis entre l'AS et la carte. Ces protocoles de reconnaissance se font sans intervention humaine. Ceci est possible grâce aux algorithmes d'intelligence artificielle.

Avant d'autoriser toute transaction, le serveur vérifie si une carte, avec ses caractéristiques physiques intrinsèques et toutes les informations qu'elle contient, fait partie de sa base de données. Le moindre écart spatio-temporel entraîne le rejet de la transaction. Cette interaction entre la carte et le serveur d'authentification a lieu au niveau de la couche physique du modèle OSI. Les autres protocoles de communication et de transport des couches supérieures ne sont pris en compte qu'après ce contact physique inévitable. Outre ces paramètres explicites, d'autres « patterns » indétectables par la compréhension humaine et invisibles aux sens humains sont stockés sur le serveur d'authentification. Par exemple, la série de Fibonacci[2] se retrouve partout dans les phénomènes naturels. Le serveur trouvera peut-être cette série dans des données génétiques et biométriques reproduites au micromètre. Par conséquent, ces correspondances entre la carte et le serveur interagissent à l'insu de l'intelligence humaine, permettant à la machine de se protéger (hypothèse H4) contre toute tentative de reproduction frauduleuse. Les mécanismes d'autoprotection et de compatibilité rendent tout accès frauduleux impossible.

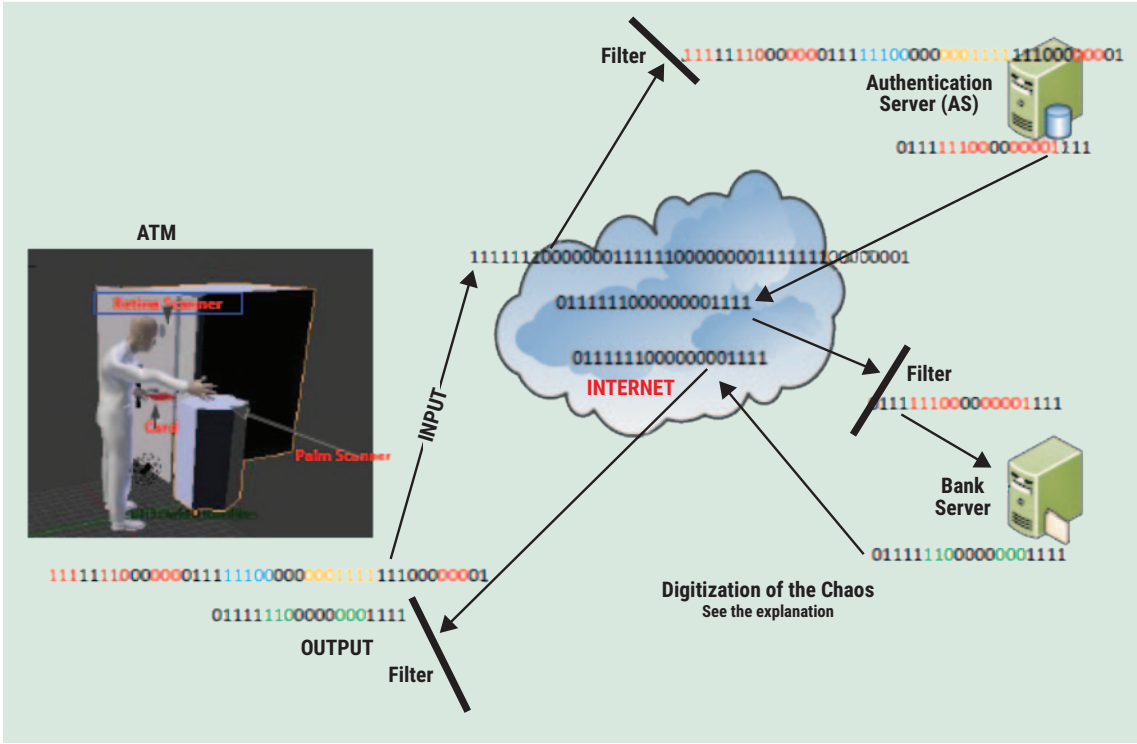
Un exemple tiré de la vie quotidienne

Pour illustrer la façon dont les processus chaotiques seront utilisés en cybersécurité, nous vous présentons l'exemple d'un retrait d'argent dans un guichet automatique **Figure 1**.

- L'entrée correspond aux données saisies par le client (bits noirs). D'autres données (bits colorés) sont ajoutées à la transaction (caractéristiques physiques de la carte, données génétiques et biométriques du client et données de localisation de l'ATM).
- Les données sont transmises via Internet comme d'habitude (bits noirs). Tout man in the middle qui analyse le flux sur Internet ne peut déterminer quels bits proviennent du client et quels bits se rapportent à des données biométriques ou proviennent de la carte ou de l'empreinte du client.
- Une fois que les données arrivent à l'AS, un filtre trie les informations en analysant chaque bit en fonction de sa fréquence (couleur). Cette opération permet à l'AS d'authentifier le client et de transmettre au serveur de la banque (BS) les données provenant du guichet automatique et entrées par le client.
- Le serveur de banque reconnaît les données du client et de l'ATM et approuve la transaction en ajoutant des informations (bits verts) à la réponse. La transaction est transmise comme d'habitude via Internet (bits en noir)

© 2019 ISACA. All rights reserved. *www.isaca.org*

Figure 1—Utiliser la Théorie du Chaos pour effectuer un tirage dans un guichet automatique



- Dans la sortie, un filtre récupère la couleur d'origine de chaque bit et le guichet automatique libère la carte et l'argent au client.

Notez deux choses importantes à propos de cet exemple de transaction :

- Les données biométriques et génétiques ne sont traitées que par un serveur d'authentification gouvernemental. (L'AS doit être un serveur d'authentification gouvernemental.)
- Tout au long de la transaction, un contact physique est maintenu entre le guichet automatique et l'AS, ainsi qu'entre le guichet automatique et le BS à l'aide d'un laser. Toute tentative de suspendre ce contact en retirant la carte annulera la transaction.

Le crime cybernétique doit payer

Tous les outils (algorithmes, circuits) permettant de réaliser cette carte numérique sont actuellement à l'étude. Théoriquement, certains existent déjà. Cette carte est conçue pour protéger l'utilisateur contre le vol d'identité et la contrefaçon. Elle utilise des données uniques et inviolables. L'empreinte de la carte, les repères spatio-temporels et les données génétiques et biométriques du titulaire sont étroitement liés. En sauvegardant ces données sur des serveurs d'authentification centralisés et sur la carte, on empêche aux données biométriques et génétiques de l'utilisateur de se retrouver dans la nature ou d'être manipulées de manière malhonnête ou incontrôlable par des inconnus et des personnes non autorisées.

L'une des objections que nous avons reçues à propos de notre système est qu'il n'y aura jamais de système inviolable. Faisons une certaine analogie médicale. Prenons la vaccination. Comme nous le savons tous, elle n'a pas éliminé la mort sur terre. Mais, nous sommes actuellement plus de 7 milliards. Et on ne ramasse plus les morts, à la pelle, au coin des rues. Comme au temps de la peste noire. Loin de nous la prétention d'avoir trouvé la panacée en matière de cybersécurité. Notre objectif est de réduire l'impunité pas d'éradiquer le crime. Quelqu'un qui force une autre

© 2019 ISACA. All rights reserved. *www.isaca.org*

personne à utiliser ses empreintes digitales sous la menace d'un pistolet ne commet pas une fraude, mais un crime. L'appât du gain, la recherche d'une certaine notoriété malsaine pourront toujours forcer quelques casse-cous à tenter leur chance. Mais à l'inverse de nos systèmes actuels, les chances d'impunité (commettre une fraude et passer inaperçu) deviennent, grâce à notre système, quasiment nulles.

Endnotes

1 Professor Messer, "The OSI Model – CompTIA Network+ N10-004: 4.1," *YouTube.com*, 18 July 2010, *https://www.youtube.com/watch?v=W438koUR04o*

2 Yash Rawat, "The Story of Maths 1 of 4 the Language of the Universe," *YouTube.com*, 13 August 2015, *https://www.youtube.com/watch?v=mJbChZrXDJE*

© 2019 ISACA. All rights reserved. *www.isaca.org*