du réseau ne peuvent pas être arrêtés pour maintenance ne serait-ce que quelques heures par semaine : ils doivent fonctionner en permanence. Les opérateurs sont aussi assez conservateurs. Les réseaux de contrôle sont en place depuis longtemps, et les opérateurs ont leurs routines qui ont fait leurs preuves. Ils se méfient de tout ce qui risquerait de menacer la disponibilité ou d'interférer avec l'exploitation normale.

Sécuriser le réseau d'ici 2020

Le NERC *(North American Electric Reliability Corporation)*, un organisme de tutelle des opérateurs du réseau américain, a édicté un ensemble de normes destinées à protéger l'infrastructure face à un danger clair et immédiat. Les entreprises de service public doivent maintenant identifier leurs dispositifs critiques et faire la preuve auprès d'auditeurs nommés par le NERC qu'ils sont capables de les protéger des intrusions.

Mais les audits de sécurité, comme les audits financiers, ne sont jamais exhaustifs. Les détails techniques audités ne sont qu'une sélection de points, et la conformité se limite à ce que l'auditeur voit.

La stratégie de protection la plus courante consiste à dresser une sorte de ligne Maginot électronique. La première ligne de défense est un « pare-feu », un dispositif à travers lequel passent tous les messages électroniques. Chaque message possède un en-tête indiquant d'où il vient, où il va, et le protocole utilisé pour l'interpréter. Sur la base de ces informations, le pare-feu laisse passer certains messages et en bloque d'autres. Les agences de certification doivent s'assurer que les centaines ou les milliers de pare-feu d'un site sensible sont correctement configurés. Pour ce faire, ils identifient quelques éléments critiques, se procurent les fichiers de configuration du pare-feu et essayent de déterminer manuellement comment un pirate traverserait le pare-feu.

Mais les pare-feu sont tellement complexes qu'il est difficile d'examiner la multitude de possibilités. Des outils automatisés seraient utiles. Notre équipe de l'Université de l'Illinois à Urbana-Champaign a développé le *Network Access Policy Tool*, aujourd'hui utilisé par des entreprises de service public et des équipes d'évaluation. Ce logiciel libre n'a besoin que des fichiers de configuration des pare-feu d'une entreprise. Il a d'ores et déjà permis d'identifier un certain nombre de chemins d'accès inconnus ou tombés dans l'oubli, que des attaquants auraient pu exploiter.

Le Département américain de l'Énergie a établi une feuille de route pour renforcer la sécurité du réseau d'ici à 2020. L'un des buts est de mettre au point un système qui reconnaît une tentative d'intrusion et qui y réagit automatiquement. Cela bloquerait un virus de type *Stuxnet* dès sa sortie de la clef USB. Mais comment un système d'exploitation peut-il savoir à quels programmes faire confiance ?

Une solution serait d'utiliser une technique cryptographique appelée fonction de hachage à sens unique. Une fonction de hachage prend un nombre immensément grand, par exemple le nombre de 0 et de 1 d'un fichier informatique, et le convertit en un nombre beaucoup plus petit, qui joue le rôle de signature. Il est très improbable que deux programmes différents et assez longs aient la même signature. Imaginez que chaque programme qui veut s'exécuter sur un système doive d'abord passer par la fonction de hachage. Sa signature est alors vérifiée par comparaison avec une liste de référence. Si elle ne correspond pas, l'attaque s'arrête là.

Le Département de l'Énergie recommande également d'autres mesures de sécurité, comme des vérifications de sécurité physiques aux postes de travail des opérateurs (des puces radio dans les badges d'identification, par exemple). Il souligne également le besoin d'exercer un contrôle plus strict sur les communications entre les dispositifs à l'intérieur du réseau électrique. La démonstration *Aurora* impliquait un programme malveillant qui faisait croire au dispositif de contrôle du générateur qu'il envoyait des instructions fiables...

Ces mesures nécessiteront du temps, de l'argent et des efforts, mais elles en valent la peine. Si nous voulons sécuriser le réseau électrique d'ici 2020, il va falloir accélérer le rythme. En espérant que d'ici là, il n'arrive rien de fâcheux. ■

L'AUTEUR

David NICOL est professeur au Département de génie électrique et informatique de l'Université de l'Illinois à Urbana-Champaign, aux États-Unis. Il est aussi directeur de l'*Information Trust Institute* de cette université.

LA MISE HORS SERVICE DE 200 POSTES DE TRANSMISSION bien choisis, soit deux pour cent du total, mettrait à genoux 60 pour cent du réseau électrique américain.

✔ BIBLIOGRAPHIE

J.-Y. Marion et M. Kaczmarek, **Boulevard du cybercrime**, *Dossier Pour la Science* n °66, janvier-mars 2010, www.pourlascience.fr/u.php?s=cybercrime

J. Eisenhauer et *al*., **Roadmap to secure control systems in the energy sector**, *Energetics Incorporated*, janvier 2006. www.oe.energy.gov/csroadmap.htm

D. Geer, **Security of critical control systems sparks concern**, *IEEE Computer*, vol. 39, n°1, pp. 20-23, janvier 2006.

Trustworthy Cyber Infrastructure for the Power Grid, projet interuniversitaire financé par le Département américain de l'Énergie : www.tcipg.org

What Is the Electric Grid, and What Are Some Challenges It Faces?, Département américain de l'Énergie, www.eia.doe.gov/energy_in_brief/power_grid.cfm

✔ SUR LE WEB

Le portail gouvernemental français sur la sécurité informatique : http://www.ssi.gouv.fr/

La vidéo de l'exercice *Aurora* : http://bit.ly/pls407-video-aurora

HISTOIRE DES SCIENCES

L'affaire de la gale : histoire d'un concept scientifique

Au XIXe siècle, les médecins accusent un jeune docteur en médecine d'avoir falsifié ses travaux pour prouver l'existence du parasite de la gale. Leur argumentation révèle tous les obstacles qui les empêchaient d'envisager cette idée.

Danièle GHESQUIER-POURCIN

Comment les concepts scientifiques se construisent-ils ? Selon l'idée la plus répandue, leur marche est linéaire et sa vitesse est fonction du nombre d'individus qui se penchent sur le problème et du temps qu'ils lui consacrent. On croit aussi généralement qu'une découverte est le fait d'un seul individu : Flemming a découvert la pénicilline, Einstein la relativité, Darwin le phénomène d'évolution et Pasteur le vaccin contre la rage. Ces croyances sont fausses. Il suffit d'examiner l'histoire d'une découverte prise au hasard pour s'en persuader. La marche des idées n'est pas linéaire. Les concepts se construisent au gré de nombreux retours en arrière et d'apports par des voies indirectes, insoupçonnées auparavant, car la diversité est le seul artisan de la progression du savoir.

De plus, l'ordre des composants de la chaîne des idées qui forment le concept est important : par exemple, on ne pouvait expliquer le phénomène d'évolution sans reconnaître auparavant l'influence du milieu. Enfin, si l'on associe une découverte à une seule personne, c'est parce que l'on porte une attention particulière à celui qui sait rassembler les idées pour reconstituer le concept. D'où viennent ces idées ? Souvent de loin, apportées par d'autres individus qui ont une part dans la construction du concept, bien que celle-ci reste ignorée. En d'autres termes, le savoir est une construction collective qui ne se concrétise que lorsque le nombre d'éléments nécessaires est en présence dans un ordre déterminé. C'est ce que nous enseigne l'étude archéologique des nombreuses strates qui constituent le concept, comme nous allons le voir ici sur un exemple représentatif de cette marche de la science : l'histoire de la maladie, plus précisément d'une « maladie spécifique », la gale humaine.

Le sarcopte de Galès : une imposture ?

Parmi les différents types de maladies connus aujourd'hui – maladies spécifiques, de carence, génétiques, etc. –, la maladie spécifique, pathologie due à un agent externe « vivant » tel qu'un parasite, une bactérie ou un virus, fut la première à être élucidée. Ce type de maladie offrait plusieurs énigmes à résoudre : l'essence de la maladie, le rôle de l'animal, les conditions de sa pénétration dans l'organisme-hôte, son mode d'action dans le déclenchement de la maladie, son mode de vie à l'intérieur du corps malade, les mécanismes de la contagion et ceux mis en jeu physiologiquement pour se débarrasser de l'intrus, les thérapeutiques susceptibles d'aider le malade à recouvrer la santé.

Une de ces interrogations était primordiale : quelle était la cause de la maladie ? La réponse à cette question conditionnait celles à toutes les autres questions, en particulier celles relatives à la thérapeutique qui, dans la maladie spécifique, se confond avec la destruction de la cause. La cause était aussi la seule façon de définir la maladie au moyen d'une propriété qui lui était spécifique.

L'histoire de la gale humaine analysée ici inclut une affaire de fraude scientifique supposée qui n'a jamais été élucidée. Au travers de cette « affaire de la gale », que nous tenterons de clarifier, se dessinera l'itinéraire des idées qui constituent le concept de gale et celui de maladie spécifique en général.

L'affaire de la gale est d'habitude présentée comme une fraude scientifique qui aurait été commise, en 1812, par un étudiant nommé Jean-Chrysanthe Galès (1783-1854) pour sa thèse de médecine, sous la direction du médecin-chef de l'hôpital Saint-Louis de Paris, Jean-Louis Alibert, spécialiste des maladies de peau. Elle a été racontée de nombreuses fois, sans qu'aucune voix se soit jamais élevée pour défendre Galès, dont la culpabilité n'a pourtant jamais été démontrée.

La gale est caractérisée par de violentes démangeaisons, des boutons et des croûtes sur la peau. Aujourd'hui, on sait que la démangeaison est due à un arthropode de l'ordre des acariens, le sarcopte. Ce parasite creuse des sillons dans le derme afin d'y déposer ses œufs, sectionnant à la fois le derme et les petits vaisseaux qu'il trouve sur son chemin *(voir la figure 1)*. Le tissu réagit en formant de petites vésicules remplies d'un liquide séreux transparent, fait de fragments cellulaires et d'un peu de sang. Si la gale n'est pas soignée, ces vésicules grossissent et se remplissent de pus, devenant des pustules. Au début du XIXe siècle, les patients traités pour la gale dans les hôpitaux parisiens se trou-