Pipelines et gazoducs potentiellement vulnérables à une cyberattaque indécelable

Eric Hazane

Août 2013 – Article n°IV.2

(Cet article a également été publié sur 01Business[1], le 14 août 2013)

Alors que le Black Hat estival (1) ouvre ses portes à Las Vegas, l'une des présentations qui y sera effectuée (2) retient déjà l'attention. Deux chercheurs de l'entreprise spécialisée en sécurité informatique *IOActive* viennent de dévoiler une possibilité de cyberattaque à longue distance (3) et sans passer par l'Internet. La cible : des modèles de sondes surveillant de nombreux paramètres et, en particulier, la pression et la température des flux transportés par pipelines et gazoducs !

Et il ne s'agit pas de modèles de niche ou exotiques mais de sondes couramment utilisées, issues des trois premiers fabricants de systèmes d'automation sans-fils (4), et positionnées à divers endroits de l'infrastructure critique de transport d'énergies fossiles (5). Elles communiquent des données critiques pour les opérations vers l'infrastructure centrale (de contrôle et de surveillance) de l'opérateur par la bande de fréquence 900MHz ou 2,4GHz.

Cependant, et c'est la procédure généralement habituelle, les vulnérabilités découvertes ont été communiquées uniquement à l'U.S. CERT dont l'une des missions est de gérer ce type de découverte embarrassante avec les sociétés incriminées. Sur les vulnérabilités, peu de détails ont filtré étant donné le caractère sensible de la découverte. Les deux chercheurs ont découvert des faiblesses malheureusement classiques et cumulatives : authentification par la même clé cryptographique (6), faible de surcroît, vulnérabilités logicielles et erreurs de configuration (7).

L'angoisse d'une attaque parfaitement invisible

Ce qui rend cette cyberattaque particulièrement inquiétante, c'est qu'elle pourrait être menée à plusieurs dizaines de kilomètres de la cible (8) et sans passer par Internet, ce qui la rendrait particulièrement indécelable. De plus, et dans la grande majorité des ICS (9), la sécurité informatique des installations est, dans le meilleur des cas, relativement moyenne sinon faible voire parfaitement inexistante.

En effet, dans le cas où des équipements de sécurité et des dispositifs de surveillance seraient mis en œuvre, ceux-ci n'ont d'autre philosophie que de contrôler les flux de données venant de l'extérieur (d'Internet, par exemple) et entrant à l'intérieur du périmètre du système industriel. Ce type de cyberdéfense, exclusivement **périmétrique**, parfaitement **inefficace** de façon générale l'est d'autant plus dans le cadre de l'attaque ici exposée.

Les deux chercheurs ont par ailleurs identifié un **scénario** qui permet d'exploiter un bug générant une corruption de mémoire qui conduit à **désactiver toutes les sondes et à couper l'installation** ! De manière très plausible, il conviendrait sans doute d'ajouter une phase de leurrage des dispositifs de

[1] http://pro.01net.com/editorial/601195/pipelines-et-gazoducs-potentiellement-vulnerables-a-une-cyberattaque-indecelable/

contrôle des paramètres en les maintenant dans un seuil d'exploitation nominal. Tout semblerait normal au centre de supervision alors qu'une ou plusieurs installations seraient entièrement éteintes. Comme lors de l'affaire Stuxnet (10), u**ne telle cyberattaque pourrait donc être conduite sans être détectée avant un laps de temps plus ou moins important.**

Des solutions longues, complexes et coûteuses

Une double problématique se pose, soulignant l'ampleur de la tâche à effectuer pour rendre la situation plus maîtrisable. Tout d'abord, il faut corriger les sondes en mettant à jour le *firmware* et en modifiant les paramètres de configuration. Une opération qui, d'après les chercheurs, ne serait pas si simple étant donné qu'il faut se connecter physiquement à chaque sonde. Sur quelques dizaines d'entre elles l'opération est relativement simple. Sur des centaines voire des milliers elle réclame une véritable organisation et possède un coût final important.

Ensuite, et c'est sans doute le nœud du problème, il faut se demander comment faire évoluer ce type d'infrastructure industrielle qui s'appuie de plus en plus fortement sur des systèmes informatiques. Et dont la conception, vieille de plusieurs décennies maintenant, n'a pas pris en compte les impacts possibles, sur la sûreté de fonctionnement, de vulnérabilités informatiques exploitables.
Le côté positif est la prise de conscience, relativement récente, de cette épée de Damoclès ainsi que l'émergence de solutions techniques adaptées (11) aux spécificités des systèmes industriels. Sans présager de la validité de ces solutions, le temps seul fera son office, soulignons qu'avant sa mise en production, toute nouvelle infrastructure ICS devrait :

- Intégrer dès la conception les principes de « *security for safety* » ;
- Etre conçue en utilisant les principes de défense en profondeur ;
- Etre dotée de dispositifs de surveillance et de contrôle des flux externes ET internes ;
- Imposer la généralisation de l'authentification forte et une gestion sensée des clés cryptographiques (12).

Les écuries d'Augias de la cybersécurité

Pour conclure, soulignons que nombreuses sont les nations à avoir identifié ce sujet comme d'intérêt stratégique car pouvant porter atteinte à leurs intérêts vitaux. Certaines d'entre elles ont même lancé de vastes chantiers, tant techniques que législatifs, qui devraient déboucher dans les mois qui viennent sur un dispositif robuste et adapté à la réalité de cette menace. Cette énième découverte vient pourtant confirmer que **les infrastructures critiques sont comme les écuries d'Augias** : le chantier est colossal, les installations à sécuriser innombrables et les vulnérabilités logicielles inconnues…proportionnelles ! Un dispositif adapté ne sera pleinement efficace que si l'ensemble des industriels concernés, ainsi que leurs utilisateurs, décident de prendre pleinement la part de responsabilités qui leur incombe. L'Etat seul ne peut pas tout y compris, et peut-être surtout, en matière de sécurité nationale.

(1) L'une des conférences internationales majeures en cybersécurité ayant lieu plusieurs fois par an à tour de rôle en Amérique du Nord, en Europe et en Asie

(2)http://www.ioactive.com/news_events_ioasis_las_vegas_2013_blackhatdefcon_carlos_penagos_lucas_apa.html

(3) Jusqu'à 40 miles soit environ 64 kilomètres

(4) donc facilement identifiables

(5) Les pipelines acheminent les flux gaziers et pétroliers des champs d'extraction vers les terminaux maritimes et/ou directement aux raffineries

(6) qui une fois cassée facilite le travail des attaquants qui peut s'introduire frauduleusement sur n'importe quelle sonde du même modèle

(7) Dans un registre différent mais avec des conséquences potentiellement catastrophiques, le lecteur pourra lire avec intérêt « De François Perrin à Stuxnet, les centrales nucléaires (cyber) vulnérables »

(8) Les chercheurs ont utilisé une antenne radio particulière

(9) *Industrial Control Systems* – Systèmes de contrôle industriels

(10) http://fr.wikipedia.org/wiki/Stuxnet#Installation

(11) Sophia, *Topological Vulnerabilité Assessment*

(12) Se référer au guide « Cybersécurité des systèmes industriels » de l'ANSSI