CHAIRE DE
CYBERDÉFENSE ET
CYBERSECURITÉ

Oil and gas pipelines potentially vulnerable to an undetectable cyber-attack.

Eric Hazane

August 2013 – Article n°IV.2

(This article was also published 01Business[1],August 1st2013)

As the Black Hat festival (1) is opening in Las Vegas, one of the presentations which will be given is already attracting attention. Two researchers from the computer security firm IOActive have just revealed a long-distance cyber-attack strategy (3) without using the Internet. The target: a type of probe which monitors many parameters and, specifically, pressure and temperature for the fluids channeled by the oil and gas pipelines.

And these are not niche or exotic probes, but widely fielded ones, issued by the three main wireless automation system manufacturers (4), and fitted onto various points of the critical energy transport infrastructure for fossil fuel (5). They communicate critical operational information to the operator's central infrastructure (control and surveillance), through the 900 MHz or 2,4 GHz frequencies.

However, in the general procedure, discovered vulnerabilities have only been communicated to the U.S. CERT, which manages these embarrassing findings with the involved companies. About those vulnerabilities, few details have leaked, given the sensitive nature of the discovery. The two researchers have found weaknesses which are unfortunately common and cumulative: same-key authentication (6), and a weak one at it, software vulnerabilities and misconfigurations (7).

The terror of a perfectly invisible attack

What makes an attack particularly frightening is that it could be launched tens of miles away (8) from the target and without going through the Internet, which would make it particularly undetectable. Moreover, in the great majority of ICS (9), the security of installations is, in the best of cases, average, when it isn't weak or outright non-existent.

Indeed, in the case security equipment and monitoring systems were installed, they have no other purpose than to control the data streams coming from outside the perimeter (the Internet, for instance) and entering within the industrial premises.This type of cyberdefense, exclusively **perimeter-based**, perfectly **inefficient** generally speaking, is even more so in the event an attack of the type stated above.

The two researchers have identified a **scenario** which enables the using of a bug which generates memory corruption, and leads to the **deactivation of all the probes and turn the installation off!** In a very plausible way, it would therefore make sense to add a decoying phase to the parameter monitoring systems by maintaining them below a nominal exploitation threshold. As it happened during the Stuxnet case (10), **such a cyberattack could be led without being detected before a certain amount of time**.

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

Long, complicated and costly solutions.

A double problem occurs, highlighting the sizeable task which awaits to place the situation under control. First of all, the probes must be corrected through a firmware upgrade and a modification of the configuration parameters. An operation which, according to the two researchers, would not be as easy as it may seem, as a physical connection to each probe is needed. On a few tens of them, the operation is relatively simple. On hundreds, or even thousands of them, it will demand solid organization and come with a heavy price.

Finally, the core of the problem lies in the future evolutions of this type of industrial installation, which rely ever more on computerized systems. Besides, the initial design is decades old and has not taken into account the consequences usable network breaches could have on the safety of operations.
On the upside, awareness has risen, relatively recently, on this Democles sword as well as on the emergence of solutions (11) technically adapted to the specificities of industrial systems. Without presuming these systems will be efficient – only time will tell – it should be stressed that before production should start, any new ICS installation should:

- Integrate the “security for safety” principles from the ground up
- Be conceived on the basis of deep defense principles
- Be fitted with surveillance and control systems for Internal AND External streams
- Impose the generalization of thorough authentication and sound encryption-key management (12).

The Agean stables of cybersecurity

In conclusion, let’s stress that the nations who have identified this subject as strategic, because liable to impact their critical infrastrustures, are many. Some of them have even launched big projects, technical and legal, which should come through in the coming months, and provide a robust system, adapted to the reality of this threat. This umpteenth discovery confirms that **critical installations are Agean stables**: the work to be done is colossal; the installations to be secured are countless, as are the unknown software vulnerabilities! An adapted system will be completely efficient only if all of the industrial contractors, and their clients, decide to take their full responsibilities. The state is not almighty, all the more in the field of national security.

(1)One of the main international conferences, which handles the theme of cybersecurity, and which takes place several times a year, alternately in Asia, North America and Europe.

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

(3)Up to 40 miles (or 64 kilometers)

(4) And therefore easily identifiable

(5)Pipelines carry gas and oil flux from the extraction fields to sea harbours or directly to refineries

(6)which, once broken, makes the assailants’ task easier, by letting them penetrate any probe of the same model.

(7)In a different field, but with potentially catastrophic consequences,the reader can read with interest «De François Perrin à Stuxnet, les centrales nucléaires (cyber)vulnérables»

(8)Researchers used a specific radio antenna

(9) *IndustrialControlSystems*

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

(11)Sophia,*TopologicalVulnerabilitéAssessment*

(12)See the «Cybersécurité des systèmes industriels» of the ANSSI.