Undocumented feature or potential vulnerability?

Evgenii Litvinov
Independent Researcher
E-mail: Litvinov.e.s@mail.ru

Abstract.

According Wikipedia: An undocumented feature is an unintended or undocumented hardware operation, for example an undocumented instruction, or software feature found in computer hardware and software that is considered beneficial or useful. Sometimes the documentation is omitted through oversight, but undocumented features are sometimes not intended for use by end users, but left available for use by the vendor for software support and development. Also, some unintended operation of hardware or software that ends up being of utility to users is simply a bug, flaw or quirk [1].

I believe that according to the definition of backdoor [2], and it refers to a special case of undocumented feature, because in both cases this information, which is known and used by vendors for software support and development.

Manufacturers of advanced sensors, gate valves, pumps, video cameras and other low-level (abbreviated as LL) automation products offer "smart" versions of their products. All of these "smart" solutions involve variability, programmability and versatility in terms of product application, as well as cost and commissioning time reduction.

Given that product variability, programmability and versatility are often achieved through the use of programmable elements, this imposes a great deal of responsibility on product manufacturers and requires vigilance on the part of consumers.

This article will not discuss individual household products in the form of smart homes, smart TVs, the Internet of Things, etc., but anyone who reads the material outlined can imagine how unpredictable any item in their home can be if the manufacturer has not shown sufficient responsibility.

Introduction.

To begin with, it is worth understanding what computer viruses are and where they come from.

In 1961, engineers Victor Wysocki, Doug McIlroy, and Robert Morris of Bell Telephone Laboratories developed small programs capable of making copies of themselves. They were the first viruses. They were created in the form of a game the engineers called "Darwin," the purpose of which was to send these programs to friends to see which one would destroy more of their opponent's programs and make more copies of itself. The player who managed to fill the others' computers was declared the winner.

In this article we will not consider all types of malware, and for brevity and simplicity we will use the term virus for all malware.

The emergence of the Win.CIH virus (Chernobyl, CIH, Spacefiller).

In June 1998, the CIH virus, which was later named Chernobyl, was detected for the first time. It got its name from the fact that it was activated only on April 26, which was the day of the accident at the Chernobyl nuclear power plant. The virus was only 1003 bytes in size. Later it was modified and resized, but it was its first appearance that went down in history and caused maximum damage.

The virus originally appeared in Taiwan at a university thanks to Chen Ing Hau, a student who created it after discovering a vulnerability on Windows 95/98/ME platforms. The virus then began to spread around the world and was found in Austria, Australia, the UK, the US, and others [3]. According to various estimates, anywhere from half a million to several tens of millions of computers around the world have been affected by the virus. According to statistics, there were about 113.5 million [4] personal computers in the world, if you compare this figure with the number of victims - it becomes clearer the damage caused.

Before Chernobyl, the maximum damage caused by viruses on a personal computer was loss of data, which could be compensated for by creating backups. The Chernobyl virus became known as the first virus that could damage not only data but also disable personal computer hardware. The emergence of this virus was a point of no return, after which users began to take computer threats more seriously.

If details of how the virus works are needed, they can be found on the TechTarget website [5] or others like it.

Was it a virus that physically damaged the computer? Probably not. The thing is that even after damaging the BIOS it was possible to restore the hardware functionality. To remove the virus, it was necessary to change the BIOS chip or to overwrite the code contained in it, which required special equipment not found at home.

For this article, it should be noted that the virus only exploited vulnerabilities on Windows 95/98/ME platforms and caused the most damage to computers with the Intel 430TX chipset. At the same time, it didn’t work on computers with NT, DOS, Macintosh and other platforms.

Background to the emergence of the virus STUXnet.

Iran's nuclear program was launched in the 1950s with the help of the United States under the Atoms for Peace program, and in 1970, Iran ratified the Non-Proliferation Treaty, limiting its nuclear program to peaceful use, and making its nuclear program subject to inspection by the International Atomic Energy Agency (IAEA) [6].

The establishment of a nuclear center at Tehran University was also one of the important results of this stage. In 1967, a U.S. research reactor with a capacity of 5 MW, with more than 5.5 kg of highly enriched uranium as fuel, was commissioned at the Tehran Nuclear Research Center. In the same year the U.S. supplied the Center with a gram amount of plutonium for research purposes, as well as "hot cells" capable of releasing up to 600 grams of plutonium annually. This was the beginning of the scientific and technical basis for the development of nuclear energy in Iran.

In 1974, the Shah of Iran promulgated a plan for the development of nuclear energy, thus setting the goal of building 23 nuclear reactors with a total capacity of 23 GW within twenty years and creating a closed nuclear fuel cycle. To implement the program, the Atomic Energy Organization of Iran was created.

Western cooperation ceased following the 1979 Iranian Revolution. The Islamic Revolution took place in the country, the Shah was overthrown, and the new government of Iran abandoned the nuclear power plant construction program. Not only foreign specialists left the country, but also a large number of Iranians involved in the nuclear project.

A few years later, when the situation in the country stabilized, the Iranian leadership resumed implementation of the nuclear program. A training and research center with a heavy water research reactor was established in Isfahan with Chinese help, and the extraction of uranium ore continued. At the same time Iran was negotiating the purchase of technologies for uranium enrichment and heavy water production with companies in Switzerland and Germany.

At the same time Iran was unfolding its national nuclear programs. In 1981, Iranian governmental officials concluded that the country's nuclear development should continue. Reports to the IAEA included that a site at Esfahan Nuclear Technology Center (ENTEC) would act "as the center for the transfer and development of nuclear technology, as well as contribute to the formation of local expertise and manpower needed to sustain a very ambitious program in the field of nuclear power reactor technology and fuel cycle technology.

For Iran, uranium enrichment is the cornerstone of nuclear energy and an opportunity to obtain its own nuclear weapons. So, the Iranians took this issue seriously. The city of Natanz was built, where the best Iranian minds were gathered and the most protected uranium enrichment plant was built. Maximum secrecy of construction, careful selection of candidates, no connection to external networks, especially the Internet, a couple of military units on the perimeter, critical infrastructure deep underground. That's how serious they were.

Of course, the construction was not unnoticed by other countries. The People's Mujahedin of Iran presented evidence in 2002 showing the Iranian government was building nuclear facilities in Natanz. In 2003, after the Iranian government formally acknowledged the facilities, the Atomic Energy Agency inspected them, finding that they had a more advanced nuclear program than had previously been anticipated by U.S. intelligence.[7] That same year, the International Atomic Energy Agency (IAEA) first reported that Iran had not declared sensitive enrichment and reprocessing activities.[8] Enrichment can be used to produce uranium for reactor fuel or (at higher enrichment levels) for weapons.

This was the situation with the Iranian nuclear program [6] and its development. In this article we are interested in the equipment of this secret plant.

The emergence of the STUXnet virus (Rootkit.Tmphider, W32.Temphid, W32.Stuxnet).

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran [9]. Although neither country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel in a collaborative effort known as Operation Olympic Games [10][11][12].

The main goal of this operation was to disrupt the operation of the facility for as long as possible. To do this, it was necessary to disable the most expensive and complex equipment at the plant - uranium enrichment centrifuges.

It is not known whether there was espionage among the workers, or controlling the delivery of equipment, or the information was obtained from open sources (from a TV report showing the operators' workstations), but the specialists knew that the entire technological process of the plant is controlled via Siemens SCADA on a Windows platform.

The main purpose of the operation was to infect the controllers with a virus, to overwrite the operating settings and to put the centrifuges out of operation (using unacceptable operating modes). Four zero-day vulnerabilities were used for these purposes.

A zero-day (also known as a 0-day) is a computer-software vulnerability previously unknown to those who should be interested in its mitigation, like the vendor of the target software [13]. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network [14].

Until now, there have been occasional debates about the possibility that it was not a vulnerability, but some kind of backdoor left by software vendors. The reader is free to take his own position on this, this article does not deal with this topic.

Stuxnet, discovered by Sergey Ulasen, initially spread via Microsoft Windows, and targeted Siemens industrial control systems. While it is not the first time that hackers have

targeted industrial systems,[15] nor the first publicly known intentional act of cyberwarfare to be implemented, it is the first discovered malware that spies on and subverts industrial systems,[16] and the first to include a programmable logic controller (PLC) rootkit [17][18].

The virus worked by first causing an infected Iranian IR-1 centrifuge to increase from its normal operating speed of 1,064 hertz to 1,410 hertz for 15 minutes before returning to its normal frequency. Twenty-seven days later, the worm went back into action, slowing the infected centrifuges down to a few hundred hertz for a full 50 minutes. The stresses from the excessive, then slower, speeds caused the aluminium centrifugal tubes to expand, often forcing parts of the centrifuges into sufficient contact with each other to destroy the machine [19].

According to IAEA reports, between 900 and 1,000 centrifuges were dismantled at the Natanz plant during the period of virus activity. All of these centrifuges had been previously installed and were operating normally.

If its goal was to quickly destroy all the centrifuges in the FEP (Fuel Enrichment Plant), Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily [20].

Using vulnerabilities and "human error," the Stuxnet virus successfully disabled about 20 percent of the centrifuges at the Natanz uranium enrichment plant, as well as disrupting the startup of the Bushehr nuclear power plant.

The virus consists of a layered attack against three different systems:

1) The Windows operating system,
2) Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows and
3) One or more Siemens S7 PLCs.

For this article it should be noted that the virus exploited vulnerabilities only on Windows platforms, vulnerabilities on the software Siemens installed in the OS, the controller software. At the same time, it did not work on NT, DOS, Macintosh and other platforms.

That is: the operating system, the software installed in the OS, the Siemens controller software. At the same time, it did not cause any damage to computers that were not involved in the enrichment process.

Present day.

An international roundtable on automation in 2019 pointed to the fact that most sensors and actuators in today's oil and gas industry are smart devices [21].

What are smart devices? Key features of definition of "smart devices" in IEC 62671 [22]:

a) The device is a pre-existing digital device that contains pre-developed software or programmed logic (e.g. an HPD) and is a candidate for use in an application important to safety.

b) The primary function performed is well-defined and applicable to only one type of application within an I&C system, such as measuring a temperature or pressure, positioning a valve, or controlling speed of a mechanical device, or performing an alarm function.

c) The primary function performed is conceptually simple and limited in scope (although the manner of accomplishing this internally may be complex).

d) The device is not designed so that it is re-programmable after manufacturing nor can the device functions be altered in a general way so that it performs a conceptually different function: only pre-defined parameters can be configured by users.

e) If the primary device function can be tuned or configured, then this capability is restricted to parameters related to the process (such as process range), performance (speed or timing), signal interface adjustment (such as selection of voltage or current range), or gains (such as adjustment of proportional band).

Manufacturers of smart LL devices need to solve the following problems:

- Increased functionality compared to non-smart devices
- Additional complexity of the component, multifunction, primary and support functions
- Potential new failure modes and hazards
- Frequent design changes by manufacturers may cause previous testing to be invalidated

What do modern manufacturers of smart devices offer? It should be noted that the development of similar and devices, software and technical solutions is a costly undertaking. In conditions of market competition, manufacturers declare commercial secrecy and limit access to information about developments. The buyer uses the product in accordance with the license agreement, without knowing what is "under the hood".

For example, specialized software allows you to perform a number of operations with LL remotely, which allows you to optimize the commissioning process. Particularly remotely, at any time, can be checked and adjusted:

- current value
- instrument scale
- measurement range
- type of environment to be measured, graduation, correction for changes, etc.
- setting of limit switches and position indicator. [21]

Considering how the STUXnet and Chernobyl viruses described above work, it is safe to say that the number of potential vulnerabilities is growing. After all, it is harder to open a door filled with concrete than one in which the locks are constantly changing.

Considering that in most cases specialized software is commercial, with closed access for reviewing documentation - the problem of vulnerability analysis becomes even more difficult. Note that in the beginning of this document, the elements of systems affected by viruses were specified - in both cases they were commercial products with closed code.

Add to this the fact that specialized software works with the PLCs that control the devices. Moreover, the network commands that LL devices require to perform diagnostic or configuration functions are often known and described. Even if they are not described in the available literature, a researcher can buy such software and a few devices. With specialized hardware, find out the signal of the required commands. Further - it is enough to write a code that simulates the issuing of a signal to the PLC control station (for example, to change the current measurement or position indicator of main valve). It is also possible to initiate the issuance of such a signal by specialized software.

Further - it is enough to write a code simulating the issuing of a signal to the PLC control station (for example, to change the current measurement or position indicator of the main valve). It is also possible to initiate the issuance of such a signal using specialized software (in case of existing vulnerability). In both cases, the LL will assume that it is in test mode, and the operator will be unaware of what is happening in the facility.

In addition, I would like to refer to a separate research by Electrical Power Research Institure, which in cooperation with specialists from various nuclear power companies in its report [23] describes the risks and the term of Undeclared Digital Content. Undeclared Digital Content, as described in the report, is also an undocumented feature.

The main problem with this research is that Electrical Power Research Institure only looked at nuclear power facilities and equipment. This may be acceptable if we want to avoid an accident at a nuclear power plant. But what if we imagine that intruders want, for example, to disable some element of the power system not related to the nuclear power plant? A cascade shutdown in case one element of the system fails would, at the very least, lead to major economic losses. What if it happens at some chemical plant or other hazardous production facility?

Conclusion.

Given the trends of viruses that have affected technical elements (first the motherboard, then the PLC) and the widespread development of smart devices, we can assume that the threat of a new virus is very real.

Judging by the two virus variants presented, we can assume that the vulnerabilities of smart devices will be exploited. This can be justified by the following arguments:

1) Modern anti-viruses are primarily focused on protecting the operating system. Activity types beyond their target surveillance are handled by Heuristics analysers. Modern anti-viruses are mainly aimed at protecting personal data and attempts to steal it by intruders. In fact, 90% of existing viruses are aimed at doing just that. If the antivirus software employs heuristic detection, it must be fine-tuned to minimize misidentifying harmless software as malicious (false positive) [23].

2) Human factors and social engineering have not gone anywhere, but have only evolved due to an increase in potential vulnerabilities.

3) Conclusion in research by Electrical Power Research Institute.

The possibility of such an incident cannot be ruled out completely. What is proposed to do to reduce the risks?

1) Ensure government (or International) regulation in the design and manufacture of smart devices.

2) Consider establishing an international automation organization. Currently there is no centralized organization, there are only the rudiments of such organizations around the world. From time to time they cooperate, but do not influence manufacturers.

References

1. Wikipedia page: https://en.wikipedia.org/wiki/Undocumented_feature
2. Wikipedia page: https://en.wikipedia.org/wiki/Backdoor_(computing)
3. 23 years of the Win.CIH epidemic. @CyberPaul on Habr.com https://habr.com/ru/companies/timeweb/articles/662740/ accessed 2 April 2023
4. Wikipedia page: https://en.wikipedia.org/wiki/Personal_computer accessed 2 April 2023
5. TechTarget: https://www.techtarget.com/searchsecurity/definition/Chernobyl-virus#:~:text=The%20Chernobyl%20parent%20virus%2C%20CIH,space%20within%20the%20P.E.%20header. accessed 2 April 2023
6. Wikipedia page: https://en.wikipedia.org/wiki/Nuclear_program_of_Iran
7. P. Clawson (2006). "Foreign Relations Under Khatami". Eternal Iran: Continuity and Chaos. Palgrave Macmillan. ISBN 978-1403962768.
8. "Implementation of the NPT safeguards agreement in the Islamic Republic of Iran". International Atomic Energy Agency. GOV/2003/40. Retrieved 24 March 2017.
9. Kushner, David (26 February 2013). "The Real Story of Stuxnet". IEEE Spectrum. 50 (3): 48–53. doi:10.1109/MSPEC.2013.6471059. S2CID 29782870
10. "Confirmed: US and Israel created Stuxnet, lost control of it". Ars Technica. June 2012.
11. Ellen Nakashima (2 June 2012). "Stuxnet was work of U.S. and Israeli experts, officials say". The Washington Post
12. Bergman, Ronen; Mazzetti, Mark (4 September 2019). "The Secret History of the Push to Strike Iran". The New York Times

13. Guo, Mingyu; Wang, Guanhua; Hata, Hideaki; Babar, Muhammad Ali (2021-07-01). "Revenue maximizing markets for zero-day exploits". Autonomous Agents and Multi-Agent Systems. 35 (2): 36

14. Compare: "What is a Zero-Day Vulnerability?". pctools. Symantec. Archived from the original on 2017-07-04. Retrieved 2016-01-20. A zero day vulnerability refers to an exploitable bug in software that is unknown to the vendor. This security hole may be exploited by crackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack.

15. "Building a Cyber Secure Plant". Siemens. 30 September 2010.

16. McMillan, Robert (16 September 2010). "Siemens: Stuxnet worm hit industrial systems". Computerworld. IDG News.

17. "Last-minute paper: An indepth look into Stuxnet". Virus Bulletin.

18. "Stuxnet worm hits Iran nuclear plant staff computers". BBC News. 26 September 2010.

19. Vyacheslav Zakorzhevsky (5 October 2010). "Sality & Stuxnet – Not Such a Strange Coincidence". Kaspersky Lab.

20. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?". Institute for Science and International Security. 22 December 2010.

21. Anniversary (to 65-annyversary of the first NPP) devoted round table of JSC "RASU": Evolution of the NPPs automation: from the relays to digital technologies", including the seminar of I&C systems section of Rosatom's NTS (Scientific and Technical Council) №1: http://nsrus.ru/meroprijatija/65let-ae/ks-rasu-2706.html "Implementation of the smart devices in NPPs I&C systems: advantages and challenges" (http://nsrus.ru/files/65NP/ppt/du-2706/rasu/Burnashev.pdf).

22. IEC 62671:2013 Nuclear power plants. Instrumentation and control important to safety.

23. Guideline on Prevention and Detection of Undeclared Digital Content. Technical report 2016. https://www.epri.com/research/products/3002008010

24. "Softpedia Exclusive Interview: Avira 10". Ionut Ilascu. Softpedia. April 14, 2010.