OFFPRINT FROM STRATEGIC OUTLOOK 7

Internet of Things:
an IT Security Nightmare

Daniel Eidenskog and Farzad Kamrani

Internet of Things (IoT) is the collective name given to products that contain electronics that have some form of connection to other systems, usually via the Internet. The number of cyberattacks involving IoT devices has increased in recent years. This, combined with a deteriorating security situation, presents a looming risk of major and wider cyberattacks in which IoT devices will be central. Sweden's national security and system of total defence are built to a great extent on the resilience of critical societal functions. Many of these have Internet-connected systems that are partially based on IoT products, making them vulnerable to cyberattacks. These systems are clear targets for antagonists. To reduce the risk of serious cyberattacks capable of disrupting critical societal functions, Sweden should have a clear strategy on cybersecurity. Sweden should also take an active role in efforts to increase cybersecurity in commercial IoT products.

A growth market with little security focus

Internet of Things (IoT) is a huge market that comprises products from a range of different sectors, such as household appliances, vehicles, building systems and industrial machines. The rate of growth of the IoT market has been high and market analysts are predicting a global increase from approximately five billion devices in 2015 to at least 75 billion by 2025. Market analysts also predict that individual consumers will own the majority of these devices. Cybersecurity is not an important criterion for this customer base, neither at purchase nor during use. New features and low prices are more often the deciding factors. In addition, there is no formal regulation of the cybersecurity aspects of IoT products and it is difficult to make the manufacturers accountable for vulnerabilities in their merchandise. In general, manufacturers have few incentives to improve cybersecurity. In many cases, this leads to products with a level of security that is far below that in many other information technology related areas.

Security is often inadequate even in IoT devices targeted at professional users. Extensive vulnerabilities have been demonstrated for example in professional-grade surveillance cameras. In several cases, these flaws have indicated a total absence of even a basic understanding of cybersecurity when developing the software for the devices.

The substantial number of IoT devices and the lack of security indicate a risk that any cyberattack that targets or seeks to take advantage of IoT products would have the potential to become a large-scale attack. Such extensive attacks would be likely to affect the infrastructure of the Internet, potentially critical societal systems and individuals.

National security is dependent on the Internet

Sweden's system of total defence relies on the assumption that normal societal services will be capable of maintaining a functioning society even in the event of a crisis or war. This applies to both military and civilian functions where disruptions and disturbances would have far-reaching operational consequences, which by extension could affect the whole of society. Fundamental societally critical sectors such as the drinking water supply, the energy supply, food distribution and communications all rely on IT systems as well as industrial control systems.

Many systems in critical sectors have connections to the Internet and build at least partially on IoT products. This puts these systems at risk of cyberattack. In the current global security climate, there is a risk that ever greater and wider attacks will be carried out against critical societal functions, where the attacks target IoT products or where IoT products are used as a springboard to amplify the attacks.

Sweden's high dependence on IT means that society is exposed to cyber-risks that would have been unimaginable only two decades ago. This dependence on the Internet as infrastructure, along with vital societal functions at risk of cyberattack, make the potential consequences of a widespread cyberattack huge.

FOI Memo 6205
Approved by: Lena Bartholdson

Offprint from Strategic Outlook 7
November 2017

FOI

To reduce the risk of serious cyber incidents and their subsequent disturbance of critical functions, Sweden must actively work to improve cybersecurity in the IoT:

Sweden should have a clear cyber strategy that aims to increase awareness and readiness. An important part of such a strategy should be to clarify the importance of the systems and components that the state does not control. The so-called proximity principle in the Swedish crisis management system puts local authorities in charge of managing a crisis. The fact that it is relatively simple to conduct a cyberattack from a distant location makes this principle ill-suited to handling a crisis resulting from a cyberattack.

Sweden should take an active role in efforts to increase cybersecurity in commercial products, for example as part of EU cooperation. Cyber security issues are basically global for all systems connected to the Internet, which means that improving cybersecurity must be pursued at both the national and the international levels. The cybersecurity situation in the private sector affects society and must therefore be part of the state's efforts in the cybersecurity arena.

Privacy is greater than the person

Another aspect of the widespread presence of IoT devices involves privacy, which by extension can also affect national security. The purpose of many IoT devices is to collect information about the user, for example in the form of places visited, health status, training habits or other activities. Devices usually send information to the manufacturer's cloud services to enable the user to easily access and use the functions provided by the services. However, these functions also give the manufacturer access to the information.

A fundamental problem is that IoT products introduce many new risks to privacy, often at a faster rate than legal mechanisms and social norms can adapt. In a world where more and more things are connected to the Internet, the cost of collecting, storing, processing and sharing data is shrinking dramatically. These privacy risks extend from simple, everyday problems, such as overprotective parents monitoring their children or intrusive marketing, to more serious cases, where governments and state actors limit the freedom of their citizens or carry out attacks against other countries.

The richness of the information that is accessible through IoT devices, combined with increased computational capacity and more effective algorithms, have created enormous opportunities for identifying, surveying, eavesdropping on and tracking individuals, as well as mapping their behaviour patterns. IoT devices often use passive methods of data collection, which means that users are usually not aware that they are being watched.

People in key positions in society risk being subjected to targeted attacks using, among other things, IoT devices. Targeted attacks against individuals are usually carried out with the assistance of well-informed and sophisticated social engineering combined with technical means. The British journalist and human rights activist, Rori Donaghy, was subjected to such a targeted attack, through a combination of social engineering and malicious code. Successful social engineering requires the attacker to have thorough knowledge of the victim, which the attacker can obtain by gathering information from diverse sources. By attacking IoT devices and potentially gaining access to large amounts of data, an attacker increases its chances of success against specific key persons.

Surveillance through bugging or tapping has long been a method for gathering just the type of information described above. One major obstacle has always been the difficulty of placing suitable listening devices close enough to the target. The dramatic increase in the number of IoT devices increases the quantity of devices that could be used for listening. In addition, the IoT devices are voluntarily put in place by the very people who are being monitored. Examples of devices that can be used for this type of surveillance are IP cameras, computers, smartphones, smart watches, wireless headsets and voice-controlled devices in homes.

Large numbers of vulnerabilities and attacks

Cyberattacks can be used to target information systems, computer networks and personal computers. The IoT – in the form of sensors, actuators, control systems and everyday objects – is increasingly interweaving the physical world with the Internet, thereby enabling new types of attack. IoT devices allow an adversary to take control of physical objects and cause physical destruction or even loss of life. The *Stuxnet* worm, which was aimed at nuclear enrichment plants in Iran, the 2015 attack against Ukraine's electricity grid and examples of researchers taking total control of a car through its Internet connection show that attacks against IoT devices encompass completely new dimensions.

The vulnerabilities in installed products are seldom addressed, since in many cases installing updates is a complex procedure that must be performed manually by the consumer. In addition, it is common for products to still be in use several years after the manufacturer has stopped releasing security updates, which makes it impossible for the consumer to avoid security defects.

Denial-of-service attacks that use IoT devices have increased in number in recent years and produced some of the most powerful disruptions of the Internet to date. In October 2016 a denial-of-service attack was directed at a core function of the Internet: a provider of the Domain Name System. It left a number of websites inaccessible to most users for several hours. Among the affected websites were Swedish government sites – krisinformation.se and regeringen.se – as well as several commercial and news services, such as Netflix, Spotify, Twitter, the BBC, CNN and Fox News. This denial-of-service attack, like several other extensive overload attacks, was based on malicious code infecting large numbers of IoT devices.

Many attacks lead to the attacker gaining complete control over an entity and its information. When the goal of the attack is the person or organisation using the IoT device, the attack can be much more subtle than an overload attack. It has, for example, been shown to be simple to hide an event by manipulating the video stream delivered by a network-connected surveillance camera.

When parts of Ukraine's electricity grid were shut down by an extensive and advanced cyberattack in December 2015, although it relied almost entirely on vulnerabilities in traditional IT systems, it also included attacks against IoT-like devices. During the attack, the attackers replaced software in certain components, causing communications with facilities to cease to function. This meant that restoring electricity distribution required manual actions to be carried out on site, and that parts of the grid could not be remotely controlled until the affected equipment had been replaced.

Destructive attacks have also occurred on the Internet using malicious code that targets certain IoT devices, leaving them unusable. There has been speculation about the actual target of these attacks. One theory is that the attackers are targeting manufacturers in the hope that they will be negatively affected by warranty claims and bad publicity. The purpose of these attacks thus being to increase the incentives of manufacturers to develop more secure products from fear of losing customers.

Attacks where the objective is to access the information in the IoT devices are often directed against individuals or organisations – opportunistically or randomly selected – from where information can be gathered or whose systems can be taken over for purposes of extortion, mapping or surveillance. Products that are increasingly present in private homes, such as network-connected surveillance cameras and baby monitors, have been highlighted in the media. Security defects have also been observed in a broad spectrum of products, such as smart televisions, insulin pumps, toys, home appliances, industrial dishwashers, thermostats, cars and sex toys.

It is extremely important that IoT manufacturers gain knowledge of the vulnerabilities of their products and rectify them. Some state actors collect information about vulnerabilities for their own intelligence activities rather than reporting them to the manufacturers or making them more generally known. This tendency is highly worrying, since there are no guarantees that such knowledge will not leak and damage the public interest, as occurred when a leaked vulnerability was used in a widely distributed blackmail virus.

Cybersecurity lacks instruments of control

There are currently no instruments for improving cybersecurity in commercial products. Customer demand in the cybersecurity area remains low, especially in consumer products as many types of attacks, such as denial-of-service attacks, do not affect the people who own the equipment. That said, the increased media focus on cyberattacks and vulnerabilities might raise consumer awareness of the impacts of inadequate cybersecurity, and with it the demands they make of manufacturers.

There are discussions at the EU level about introducing a “trusted IoT label” for IoT products that meet certain security requirements. This is meant to build on the same principle as the energy labelling of domestic appliances, where the specifications are clearly presented for the consumer to direct them towards safer or more energy-efficient products.

An alternative route would involve legislation and regulation. One possibility would be to design regulations similar to the system of mandatory CE-labelling of products sold within the EU. CE-labelling places greater responsibility on the manufacturers and importers of products, this has generally worked well, although some fraudulence still occurs when products are CE-labelled even though they have failed to meet the regulatory requirements.

As long as the current lack of incentives for producers persists, however, there is every indication that the problems caused by inadequate cybersecurity in the IoT arena will continue for the foreseeable future. As the number of installed IoT devices increases, the consequences of insecure IoT will continue to increase.

Further Reading

Farzad Kamrani, Mikael Wedlin and Ioana Rodhe, *Internet of Things: Security and Privacy Issues*, 2016. FOI-R--4362--SE.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Phone: +46 8 5550 3000
Fax: +46 8 5550 3100
https://foi.se/en.html