Chapter 1

Introduction

In September 2007, Israeli jets bombed what was suspected to be a nuclear installation in Syria. Apparently, the Syrian radar that was supposed to warn about the attacks malfunctioned in the critical time interval prior to the Israeli attacks. Eventually, an alleged leak from a US defence contractor suggested that a European chip maker had built a kill switch into its chips. The radar may thus have been remotely disabled just before the strike took place [1].

Whatever the real truth might be, the discussions around the bombing of the Syrian nuclear plant highlight a profound difference between electronic equipment and any other type of technology. When you buy an electronic device, you enter into a long-term relationship with the people and companies who developed and produced it. Their power over the equipment prevails long after you have bought it, even when you believe to be the only one who operates it and even while it is under your physical control. The relation between makers and buyers of information and communications technology equipment is thus very different from most other buyer–vendor relationships.

Three properties of electronics created this situation. First, the functionality that is there when the equipment is shipped is largely invisible to the customer. Second, a stream of software updates gives the manufacturer the ability to change the operation of the equipment long after it has been bought. Third, since most equipment is connected to the Internet, the manufacturer has the power to receive information from the equipment and even to operate it remotely.

This begs two important questions. First, for what could a manufacturer want to use its powers? Second, what means do we have to control the actions of the manufacturer? In this chapter, we give a high-level overview of these questions. We cite cases in which the position as the manufacturer of electronic equipment was misused to make the equipment work against the interests of its owner and we explain why the problem of protecting against untrusted vendors is different from that of protecting against third-party attacks. Finally, we relate the problem to questions of national security and international trade.

1.1 A New Situation

The trading of tools between tribes is probably as old as toolmaking and trade themselves. Early artefacts were perhaps arrowheads, axes, and knives made of stone and their exchange increased the hunting or fighting capability of the parties taking part in the transactions. The quality of these early tools was easy to verify and clearly no one feared that the tools themselves could turn against their owner.

As history evolved, the tools became more complex. Consequently, understanding the quality of a product became a more complex task. Still, as recently as 50 years ago, the fear that the tools you bought could be made to turn against you was practically nonexistent. Furthermore, if you feared such attacks, countermeasures were easily available. Equipment could be disassembled and understood and any exploitable weakness or malicious functionality ran a very high risk of being detected.

Today, the situation has changed. To a rapidly increasing degree, societies, organizations, and individuals base their lives and well-being on electronic tools and infrastructures. These electronic devices and tools are built with a complexity that surpasses human capacity for analysis. This is obvious from the fact that we are frequently surprised by what the devices we buy actually do. ‘Oh, I didn’t think it could do that!’ is a reaction most of us have had to our mobile phone.

It is not only as private consumers that we are losing our ability to check what our devices really do. The complexity of modern computer systems is so great that, even for the people developing them, their behaviour is impossible to fully control. For instance, we do not expect computer systems to be free of design or programming faults anymore, because we know that building fault-free systems is nearly impossible. This is accepted to the extent that no one will buy complex equipment without a support agreement that the vendor will provide software updates to correct programming mistakes as they are identified.

1.2 What Are We Afraid Of?

The reason for such support agreements is that buyers are not expected to find the bugs themselves. Neither are they assumed to be able to correct them, regardless of the resources their organization may have. However, if the buyers of equipment are no longer expected to even understand what the electronic system they have bought can do, this has serious implications. It means that the vendor of the equipment has the power to make it do things that are not in the interest of its owner. The vendor could make the equipment turn against its owner without the owner ever finding out.

This begs the question of what a dishonest vendor could possibly do. The exact answer will vary depending on the motivation of the dishonest vendor, but the actions we need to be concerned about are the same as those we fear from third-party cyber-attackers. We fear that they will carry out espionage and surveillance to get hold of confidential information, from either companies, private persons, or nation states.

We fear that they will sabotage key equipment, either permanently or temporarily, to achieve some objective. Finally, we fear that they can commit fraud. Do we have stories of equipment manufacturers using their position as vendors for espionage, sabotage, or fraud? Yes, we do. Some examples are documented beyond doubt, some are made credible through circumstantial evidence, and some are just fear-based speculation.

One well-documented case of espionage is that the routers and servers manufactured by Cisco were manipulated by the National Security Agency (NSA) to send Internet traffic back to them. This case is well documented through documents made available to the press by Edward Snowden [3] and it is therefore a solid example of espionage done through an equipment provider. There is no evidence that Cisco was aware of the NSA's tampering, but the example is still relevant. When you buy equipment from a provider, you have to trust not only the provider, but anyone who is in power to change the equipment. To what extent Cisco itself contributed is therefore beside the point.

Another case of privacy-invading espionage is from November 2016. Kryptowire,¹ a US-based cybersecurity company, found that several models of Android mobile devices contained firmware that transmitted sensitive personal data to a server in China without disclosure or the users' consent [5, 7]. The code responsible for these actions was written by Shanghai Adups Technology Company, a Chinese company that allegedly provided code for 700 million phones, cars, and other smart devices. The phones were available through major online retailers and they sent user and device information to China. The leaked information included the full body of text messages, contact lists, and call history, with full telephone numbers. The intention of this surveillance is unclear, but Adups explained that the code was made for a Chinese manufacturer. One of their lawyers described its presence in phones sold in the United States as a mistake.

An example of fraud is the Volkswagen case, in which electronic circuits controlling a series of diesel engines reduced engine emissions once they detected they were being monitored [2]. This was deliberately done through the functionality of an electronic component put into cars by their manufacturer. Volkswagen misled American authorities into issuing approvals of the engine series, even if, under ordinary use, the engines emitted nitrogen oxide pollutants up to 40 times above allowable US limits. Volkswagen also misled buyers into thinking that the cars were environmentally friendly. This case was eventually detected by the authorities, but the important observation here is that the detection was not the result of analysis of the digital component; it was the result of analysis of the highly analogous behaviour of the diesel engine. The engineers who committed this fraud did so under the assumption that what they had done on the electronic chip itself would not be discovered.

Examples of sabotage from vendors of electronic equipment are fewer and less well documented. The event that we started the chapter with – when the Syrian radars malfunctioned just before an Israeli airstrike on a nuclear installation in 2007 – has

¹Kryptowire is a contractor of Homeland Security. The discovery reported here was reportedly done outside of these contracts.

not been documented beyond doubt. In the aftermath of the event, there was intense speculation of what had happened, but no real proof has been put forward.

The merits of such speculation are, however, not important. The crucial observation is that we seldom have hard evidence to dismiss such arguments. The motivation of the vendor of the equipment to include unwanted functionality in the Syrian radar is clear. Its technical ability to go through with it is quite obvious and the chances the Syrians had to uncover the problem before it was too late appear to have been slim. Even in the absence of verified examples, the inclusion of kill switches that render equipment useless through a predefined external trigger is too powerful a concept to be ignored.

1.3 Huawei and ZTE

Discomforting as the above examples are, the most heated debate on trust in vendors of electronic equipment relates to Huawei and ZTE. These two Chinese companies are becoming increasingly dominant in the telecommunications market. Because of the vendors' Chinese origin, countries such as the United States, Australia, and Canada have repeatedly questioned their trustworthiness and objected to including their equipment in national infrastructures. The distrust is mainly motivated by Huawei's possible ties to the Chinese military and thus to the Chinese government.

Open political debate on how to handle the question of whether to trust Chinese vendors has taken place on three continents. In October 2012, the US government released a report by the US House of Representatives' Permanent Select Committee on Intelligence [10]. The report presented an analysis of the threats associated with remote equipment control, especially in the case of a cyberwar, and strongly urged that US firms stop doing business with both Huawei and ZTE. Australia has echoed the same concern. In 2011, the Australian government barred Huawei from bidding for the country's national broadband network project, based on security concerns associated with Huawei's hardware [12]. In Europe, Huawei, along with its smaller rival ZTE, hold almost a quarter of the European telecommunications equipment market. According to the European Commission, this strong market position poses a security risk because European industries ranging from healthcare to water utilities are becoming reliant on Chinese wireless technology [9]. In the United Kingdom, a parliamentary committee commented that it was "shocked" at the government's failure to monitor Huawei's activities and called its strategy for monitoring or reacting to cyberattacks "feeble at best" [11]. In France, telecommunications executives say the government generally discourages them from buying Chinese equipment for their core networks, but not for cell phone base stations and radio equipment [11].

It is important to note that there is no evidence or indication that Huawei, ZTE, or any other Chinese vendor, for that matter, has misused its position as a vendor of equipment against any of its customers; there are only suspicions, mainly based on Huawei's possible ties to the Chinese military and thus with the Chinese government. Therefore, some would categorize the suspicions as unsubstantiated fear. To us,

however, the discussions themselves are important. From their mere existence, we can draw three very important conclusions, as follows:

1. It is critical for a modern society to be able to rely on its electronic equipment and infrastructures. All of society's critical functions, such as healthcare, financial stability, water supply, power supply, communication, transport, and ability to govern a state in a situation of national crisis, depend on them. The need to have an understood level of trust in critical infrastructure is the reason the discussions on Huawei and ZTE have reached the level of national security politics.
2. Investigating what electronic equipment does or can do is highly nontrivial. If it were easy, we would not need to discuss how much we can trust such equipment; checking and verifying it would suffice.
3. Few countries have the ability to design and produce the electronic equipment for their critical infrastructure entirely by themselves. In other areas, governmental regulatory bodies impose rules on systems of critical importance to national security. If designing and producing critical equipment nationally were a viable path, it would be an obvious solution to the problem.

The three observations summarize the motivation for this book. The trustworthiness of electronic equipment is paramount and we cannot choose to design and produce all aspects of this equipment ourselves. The question we then need to answer is how we can check and verify the equipment and how we can build well-founded trust.

1.4 Trust in Vendors

Trust in a vendor may have a varying foundation. We can choose to trust a vendor based on a long-term relationship or based on the vendor's reputation. In both cases, our trust is based on their previous actions. We could also base trust on our capacity to verify the contents of the vendor's equipment. In this case, the decision to trust rests on our belief that malicious intent by the provider will in some way be visible in the product and that we will be able to detect it. These bases for trust are often used in the discussions regarding Chinese vendors of telecommunications equipment. Unfortunately, as we shall document in this book, these arguments do not hold water.

When we discuss our fear of what equipment providers could do, our concerns will in all cases be related to what they could possibly do in the future. A key observation is that a provider could change tomorrow the properties of equipment we bought and installed today, since hardly any complex electronic equipment is sold without a support agreement. A steady stream of security updates will come from the provider of the equipment. For fear of being attacked by a third party exploiting the security holes closed by the updates, we will dutifully install them. These updates will have the power to change the operation of the equipment itself, even to the extent of performing actions against our interests. Consequently, the question of trust in

a vendor has a timeless perspective. We may have every reason to trust a vendor based on experience with the company in the past. We may also be correct in that the vendor is currently to be trusted. Unfortunately, our need for software updates makes any change in the vendor's trustworthiness influence the trustworthiness of all the equipment ever bought from that vendor. Therefore, when we ask ourselves if a vendor can be trusted, we have to ask ourselves if we believe the vendor will remain trustworthy for the entire lifetime of the product we are buying.

1.5 Points of Attack

So far, we have somewhat inaccurately discussed the notion of a vendor as if it needed no further explanation. There are, however, many types of vendors and each type has a different potential point of attack and a different potential to cause harm [4]. Some provide pieces of intellectual property to be integrated as a small part of a silicon chip. Others may build the chip itself or the printed circuit board onto which the chip is welded. Some vendors provide the hardware abstraction layer or the operating system running on top of the hardware and a large group of vendors provide applications running on top of the operating system. There are system integrators synthesizing hardware, operating systems, and applications into a complete product and there are service providers providing communication or data centre services. Most vendors of electronic equipment are also buyers of software or electronic components needed to build what they eventually sell.

The most critical buyer–seller relationship is that between an operator of critical infrastructure – such as telecommunications, power grids, and cloud facilities – and the provider selling the equipment for this infrastructure. Throughout the book, we will often assume a vendor–buyer relationship in which the values at stake are high. Furthermore, the equipment bought is assumed to be a fully integrated physical product containing hardware, firmware, an operating system, drivers, and applications. Still, most of this book is of relevance to all buyer–seller relationships in the computer business, including buyers and sellers of components that go into finished products and buyers of electronic services provided by operators of infrastructures.

1.6 Trust in Vendors Is Different from Computer Security

Computer security has been a research field for decades. We should therefore ask ourselves whether the problem we address in this book raises new questions of computer security that have not previously been investigated. To answer this question, we have to extract and express some underlying assumptions in most work on computer security.

An often-cited definition of computer security is that of Peltier: [8]: *Information security encompasses the use of physical and logical data access controls to ensure*

the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets.

This definition or variants thereof has formed the basis of security research for decades. Its weakness – and thus the weakness of most security research – is that it focuses on “physical and logical data access controls”. Although this phrase does not explicitly exclude the scenario in which the vendor of the equipment is the perpetrator, it has led to the almost ubiquitous and most often implicit assumption that the buyer and the producer of equipment are collaborating in defending against a third-party wrongdoer.

Out of this assumption comes a set of approaches that are not valid for our case, in particular, those for stopping malicious software, or malware, from entering your system. If the wrongdoer is the vendor, the malware may be in the system from the moment you buy it and stopping it from entering later therefore makes no sense. Another assumption is related to the mechanisms for detecting malware infections. These methods assume there is a noninfected golden sample for comparison. Since this golden sample has to be provided by the vendor, the notion of being noninfected is doubtful if you do not trust the vendor [6]. Yet another mechanism is based on building cryptographic security into hardware. A Trusted Platform Module is a piece of hardware that can be used to verify that the configuration of software and hardware on a system has not been tampered with. In our case, this will not help. We inevitably need to ask the question of who made the cryptographic module and to what extent the maker can be trusted. In summary, four aspects make our problem different and far more difficult to handle than the scenarios addressed in mainstream security research:

- When malware is already in the system at the time of purchase, stopping it from entering is futile.
- When there is no golden sample, it is not possible to detect tampering by comparing a system to a known healthy system.
- Built-in security mechanisms in system chips, operating systems, or compilers are in the hands of vendors we may not trust.
- The malicious actions of the system can be performed anywhere in the technology stack, from low-level hardware to software controlling the user interface.

The implications of these differences will be discussed in this book. We will go through the different computer science specialities and analyse the extent to which the current state of the art contains knowledge that can help us solve our problem.

1.7 Why the Problem Is Important

The importance of a problem should be measured by its consequences. Before we spend time delving into the finer details of controlling an untrusted vendor, we therefore need to understand the consequences of not being able to do so. It turns out that

there are consequences for the buyer of the equipment, the vendor of the equipment, and for society at large.

The consequences for the buyer of the equipment are the most evident. If you need to invest in equipment for critical infrastructure in your country, you will be concerned with everything that can go wrong. You also need to think through scenarios of international crisis and even war. The discussions related to the Chinese companies Huawei and ZTE are examples of this challenge. Although no international consensus is reached on how to treat untrusted vendors, the discussions themselves reveal that the problem is considered important to the extent that it has reached the level of international politics.

The vendors, on the other hand, see the problem differently. Assume you are in the business of selling equipment and that you are completely trustworthy. Still, you lose contracts because there is no way you can prove beyond a doubt that your equipment is trustworthy. This is the situation in which the Chinese providers find themselves. No matter how understandable the worries of Western countries are, it is evident that it is extremely important for Huawei to be able to demonstrate the worries are groundless.

Finally, the difficulties we have in building a solid basis for trust between vendors and buyers of electronic equipment are a potential obstacle for international trade and cooperation. The internationalization of trade since the Second World War has fuelled financial growth in most societies around the world and this trade has been argued to be an important factor in the formation of trust between nation states. This trust has, however, never been blind, in the sense that the parties could not control the quality, properties, or actions of the goods that were traded. The lack of a solid basis for trust between buyers and sellers of electronic equipment therefore not only is a problem in the relation between the buyer and the seller, but can also be seen as a factor limiting the trust needed to grow international trade.

1.8 Advice for Readers

The topic of this book should be of interest to several groups of readers. One is security experts who need to understand the vulnerabilities implied by the vendor–buyer relationships they are a part of. Another is security researchers who need to understand the limitations of the state of the art, when a system must be defended against different adversaries from those previously considered.

An often overlooked but important group of stakeholders for this problem is the decision makers in nation states, public bodies, and large companies. Their need to understand this problem is huge, since they are the ones ultimately making the decisions that establish the type of customer–vendor relationships on which we focus. More often than not, these people are not educated technologists.

Therefore, We have made an effort to make this book readable and useful for all groups. Technologically savvy readers are advised to read the entire book from start to finish or to focus on the chapters of special interest between Chaps. 4 and 10.

Interested readers without a technology background should gain an informed view of the problem at hand by reading Chaps. 1–3, the conclusion of Chap. 4, and, finally, Chap. 12.

References

1. Adee, S.: The hunt for the kill switch. *IEEE Spectr.* **45**(5), 34–39 (2008)
2. BBC: <http://www.bbc.com/news/business-34324772>
3. Greenwald, G.: No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State. Macmillan, Basingstoke (2014)
4. Jøsang, A.: Potential cyber warfare capabilities of major technology vendors. In: 13th European Conference on Cyber Warfare and Security ECCWS-2014, pp. 110–115 (2014)
5. Kryptowire: Kryptowire discovers mobile phone firmware that transmitted personally identifiable information (PII) without user consent or disclosure. http://www.kryptowire.com/adups_security_analysis.html
6. Lysne, O., Hole, K.J., Otterstad, C., Aarseth, R., et al.: Vendor malware: detection limits and mitigation. *Computer* **49**(8), 62–69 (2016)
7. New York Times: Secret back door in some U.S. phones sent data to China, analysts say. <http://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html?smprod=nytcore-iphone&smid=nytcore-iphone-share>
8. Peltier, T.R.: Information Security Risk Analysis. CRC press, Boca Raton (2005)
9. Reuters: Exclusive-EU threatens trade duties against China's Huawei, ZTE-sources. <http://www.reuters.com/article/us-eu-china-huawei-idusbre94d0rx20130515>
10. Rogers, M., Ruppertsberger, D.: Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE. [http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zteinvestigativereport\(final\).pdf](http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zteinvestigativereport(final).pdf)
11. The Wall Street Journal: U.K. raises cybersecurity concerns over Huawei. <http://online.wsj.com/article/sb10001424127887323844804578529141741985244.html>
12. ZDNet: Don't let Aus fall into US-China security fight: Huawei. <http://www.zdnet.com/dont-let-aus-fall-into-us-china-security-fight-huawei-7000006282/>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.