02

THE TECHNOLOGY BEHIND CYBERSECURITY

NIELS TEN OEVER, ARTICLE 19

INTRODUCTION

Security can be defined as a state of being free from danger or threat. This can only be achieved if one has a level of control over the environment in which one is operating. In terms of systems security this would mean that one has control over the processes that are executed on a specific system and one has clear permissions for different (sets of) users. So nothing or noone does something that is not expected. To have this level of control over a system, one needs to understand what processes are running on a system and what these processes do. One also needs to have the trust or understanding that these processes will not all of a sudden execute operations that you do not expect them to perform, and if they might behave out of the ordinary, these processes should not have access to essential resources or operations. So security is in large part about restrictions.

THE WHAT – WHAT IS THE TOPIC ABOUT?

There are generally three levels of concern: Software, hardware and users. Software are all the programs, applications and operating system(s) that are running on your device, these are practically machine readable instructions that are performed by the hardware. The hardware is all the physical elements that constitute a computer system.

Both software and hardware can contain vulnerabilities, undocumented ways that could enable third parties to have access to your computer, often in a way that is difficult to detect. There are intentional vulnerabilities, which are called 'backdoors', that enable third parties to have access to the system or execute specific task. But there are also many unintentional vulnerabilities, which can be mistakes by developers, or an implementation that was secure when it was programmed, but because of new developments isn't secure anymore. There is a lively market in undiscovered exploits, which are called zero-days[12]. These are called zero-days because it has been zero-days that the vulnerabilities are known by the public. This is why a good understanding of the hardware and software and the expected behaviour is important.

Finally users are a crucial part to cybersecurity. Users don't like to be limited and often work around security barriers that have been put in place. For users, security often feels like a hurdle, like using strong passwords and replacing them every

12 http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/

three months. So they write their passwords on post-its, or re-use the same login and password they might use for a webshop (with very low security standards).

You might think that this only happens to home computers, but unfortunately bad security practices can be found everywhere on the Internet, ranging from very big routers to systems that control power plants. What makes doing security on the open Internet so hard is that what is secure today, might be insecure tomorrow. Vulnerabilities in crucial parts of software are found everyday. As previously mentioned, there is a market for zero-days, where some of the main customers are governments. This new trend stimulates security researchers to not disclose the vulnerabilities to the developers of the software, but rather to keep it hidden, which in the long term leads to a more insecure biotope of software.

For many parts of civil infrastructure where the net is used, these systems are called Industrial Control Systems (ICS), the large implementation of this are Supervisory Control and Data Acquisition systems, SCADA in short. These are used to control water purification plants, oil pipelines, power plants, and much more. By using the Internet, these networks are exposing themselves to attackers, but on the other hand it provides for ease of use and allows for remote control and monitoring. And this is exactly where its weakness lies. By being connected to the Internet it allows for third parties to try to get access to the systems; to prevent this, the systems need to be carefully configured and regularly updated. Unfortunately this is often not the case; people are not upgrading their servers, weak passwords are being used and sometimes the systems can be accessed via the browser through an insecure connection. It is often the perception that when a system is in place, no further work is needed, but maintenance, monitoring, updates and upgrades are an essential part of having a secure environment. And here we're not even talking about advanced targeted attacks.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The issue of security becomes harder when we add Internet to the mix, because the system one tries to secure is much more exposed. To make a system more secure practically means to limit its possibilities: the fewer options there are, the fewer things can go wrong. But this is the opposite of what we want for the Internet, especially one that strengthens human rights: the Internet became the important infrastructure for freedom of expression and access to information that it is today because its use is not limited to certain things, its aim is connectivity, and the Internet Protocol is the tool to realise this. This opens the endless opportunity for innovation, and possibilities but also a lot of risks.

THE WHO – WHO ARE THE MAIN PLAYERS?

In the guidelines for secure operations of the Internet (RFC1281) the IETF states that the Internet is a voluntary network, operated on a collaborative basis, and that everyone on the network has their own role to play in security:

- **Users** are individually responsible for understanding and respecting the security policies of the systems and they have a responsibility to employ available security mechanisms and procedures for protecting their own data.
- **Computer and network service providers** are responsible for maintaining the security of the systems they operate. They are further responsible for

notifying users of their security policies and any changes to these policies.
- **Vendors and system developers** are responsible for providing systems which are sound and which embody adequate security controls

Responsibilities are found on every level, but these are guidelines which are not always followed up. Most cybersecurity risks are caused by badly administered systems. This means security updates that have not been done, bad password management, opening of e-mail attachments with viruses. Bad administration of systems allows for botnets to take over your computer to do an orchestrated attack on thousands of computers at the same time.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The trade in zero-days, the development of malware, and the practice of weakening standards are no precision attacks on specific targets, as one might think. Once attacks are 'out in the wild' they often get copied and partially re-used, both when it's a 'trick' or a piece of software. Even if we look at one of the most advanced attacks we've seen in recent history, the Stuxnet worm, which was aimed at an Iranian power plant, made its way across the Internet to India, Iran, Indonesia and back to the US. Technology democratises: once a code or practice is out there, one cannot get it back. This is why the development of malware and the trade in zero-days (instead of informing the providers of the vulnerability) are both such dangerous practices, which might even backfire against the party that developed it.

There is a world to win when it comes to cybersecurity. There is an increasing cooperation in this field, but more can be done: governments could standardise and support penetration (vulnerability) tests of its own systems, those of important industry players and critical infrastructure and report security vulnerabilities to developers. Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) could be strengthened, and knowledge on digital security and best practices should be mainstreamed, so that no one leaves their digital house, factory or government building with the keys in the door.