Paradoxes in Information Security

Introduction

In this article, we approach information security from a novel perspective as we examine its unintended ramifications and its paradoxes. Information security and cybersecurity are necessities of modern societies. Simply put, services which are based on information and communication technologies would not function without information security. Thus, information security can easily tend to be thought of in only positive terms, as it ensures and facilitates our way of life. Furthermore, people rarely complain of information security being *too* sturdy. So the case between Apple and the FBI, in which the FBI finds the robustness of security in the iPhone software problematic, is an uncommon case [1]. It is much more common for problems pertaining to information security to be related to vulnerabilities and weaknesses in information security.

However, there are many paradoxes that come with information security. Fundamentally we argue that information security seeks to exclude interruptions to the system it protects, yet it is in fact itself an interrupter that makes the system different. First we describe information security in general, along with its significance in terms of the functioning of society. In other words, we go through the positive side of information security. Then we discuss information security in a slightly more theoretical manner. Our purpose is to discover what in fact information security is by looking into what it does. Then we start to go through its paradoxes.

Dependence

For some time now, information systems have constituted and created the central communication hubs in our societies. With the rise and popularization of the World Wide Web in the 1990s, networks even become a metaphor for the entire society [2]. At the time, information was already quite agile and mobile, but devices were not. Now the use of smart devices, which was a subject of speculation in early 1990s [3], have entered into everyday life and become intertwined with the domain of the social. Furthermore, it is not only the devices that people carry but also everyday objects that have gained the capability for net connection. However, as more and more things can compute and communicate, they become problematized in terms of security. For example, cars and smart devices in the home [4] have embedded information systems that can be vulnerable [5]. In other words, the world is full of different information systems that are also becoming more ubiquitous, pervasive and social. We literally live with, through and on technology.

As all the crucial aspects of modern societies – from monetary transactions and energy supply to communication between people – depend on information technology, the smooth functioning of these surrounding information systems is required. Furthermore, since societies and everyday life are dependent on information systems, information security is needed. Because of this dependence, it is understandable that usually information security is discussed in very positive terms.

What is information security?

So, in modern societies we are all dependent on – or live in surroundings that are dependent on – information security. However, the question still remains of what we are dependent on: what is information security? Usually with information security three central words are mentioned: confidentiality, integrity and availability [6]. Confidentiality and integrity are based on the idea that only an authorized user should be able to access (to see) and edit protected information. Integrity pertains to the consistency of information. Information should not change unless an authorized user modifies it. Availability refers to the requirement of accessibility. In other words, information should be available (and modifiable) when needed by authorized users.

Achieving a state of security is never a straightforward process as information security is a relative matter in several ways. The concept of information security is so overarching that it can be approached from so many angles: it has been called a process, connected to awareness, can be approached in terms of philosophy, and there is the social side of information security [7]. Security is based on relations and ownership. It is a question of who the authorized user is, who has ownership of certain information and what the authorized user desires to do with it. Because security is connected to users' desires, it means that there is no way of knowing, for example, whether the structure and status of certain files is secure or not merely by examining the files themselves. In other words, by looking at the registry, files, and processes of a computer, you cannot say whether the computer is secure or not. In order to assess how secure something is, you need to know what the owner of that computer wants, what he or she desires. Let us clarify this through an example. Think of a text file that you have written and saved on a mass storage device. Later, the file is erased and the text is gone. The question is: is this a good or a bad thing? Did deleting the file serve information security? There is no way of telling whether the action is benign or malicious without knowing what the owner of the file wants. Again, this assessment cannot be based on the mere status of the file (deleted, not deleted); the user's desire (and/or organizational information security policy) has to be included. However, and importantly, the external desire is not an absolute in the sense of always being the same. Of course, users usually resemble each other, which makes users' desires sometimes look as though they are absolute and universal. For example, most email users do not want to receive spam. However, conceptually, desire is always open.

Despite the relativity of security, we can define information security by what it does; namely, it protects the order of relations [6]. Thus, in our example above, information security seeks to protect the relation between the user's desire and the file. In the larger context of a modern society dependent on information systems, this means that there is a desire to ensure that information systems function smoothly (which is one objective of information security).

Paradoxes

Although all information security is nowadays mainly warmly welcomed, this has not always been the case. In the past, in the golden age of hackers ("hacker" referring here to a technology enthusiast desiring to develop the systems), computers were rare and access to them was thus very limited [8]. However, as the hackers wanted to try things out with computers, the desire to remove any obstacles (including physical locks and passwords)

emerged. The idea of freely flowing information was developed. Statements along the lines "the source code should not be hidden" started appearing [9]. Information security has been considered to slow down the flow of information but also to impede development. However, this is a skeptical view on information security rather than a paradox of information security.

Let us move to the actual paradoxes. As we have discussed, information security seeks to prevent systems being interrupted. For example, information security makes sure that monetary transactions are not interrupted. However, paradoxically, information security itself works through interruptions. As it prevents external interruptions, distortion and distraction, it in fact generates them. For example, one such interruption generated by information security is the request for a password and user name [7]. Use a web-based service and you are asked for credentials. In simple terms, this enquiry is a stoppage, an interruption. The user is cut off from their normal flow of action. The same applies to security updates which require a restart of the system. Interruptions due to a restart occur on a frequent basis.

These are not mere halts, but a drain of energy. The information security procedure – the request for a username and password – steals a bit of the user's energy. It involves the user, makes them give information in order to analyze and identify the user. We argue, in fact, that information security uses the user. Furthermore, the consumption of energy goes beyond the user, as the procedure steals energy from the processors running the information systems (e.g. the server on which the service is executed and the user's device that is connected to the server). Information security is an additional and external – even excessive – system, which resides parallel to the actual system. Slightly differently put, information security uses the energy of the system that it is supposed to protect. Thus, entering a PIN code, passwords, or placing one's finger on the scanner are all external jobs that do not have anything to do with the main task.

Of course, it can be argued that the system can be made to remember passwords. The fingerprint scanner can be deactivated. The entire system can be configured in such a way that no passwords are required. However, as the energy drain is avoided, the level of security is also lowered. Alternatively, the interruption has changed its form. If a program that remembers the passwords and hides them behind a master password is used, then interruption comes in the form of the installation of that program. In addition, this program then consumes some of the device's resources.

Information security is based on analysis and control [7]. However, every analysis is an interruption in itself. The interruption of information security is not pointless or random but overarching: interruption concerns all the entities that come into contact with the system that is under protection. Every entity is analyzed and interrupted. It makes no difference whether you are a legitimate user or a malicious hacker. Both are analyzed. Equality is generated in a strange way. The difference comes after the analysis. Then, the user is either authorized (allowed use of the system) or rejected (denied access).

Information security functions as a maintainer of order. However, paradoxically, in order to keep the existing order of the system, the order is altered by information security [6]. For

example, a security program installed on a system reorganizes processes and reroutes the flows of information within the system that it protects. In order to monitor network traffic, an additional loop is required. In order to keep viruses excluded, a virus scanner is installed. However, these all drain energy – processing cycles – from the actual system. Information security seeks to protect an order, yet it changes that order.

To put it slightly differently, information security is a reorganizer, an additional element that adds complexity to the system. In order to protect information and information systems from distractive and interruptive entities, information security establishes an order that is always distractive and interruptive in terms of the main functioning of the system. Usually the interest has been in how malware, for example, slows down computers [10]. However, the same question can be posed to information security. For instance, absolute and overarching network monitoring would require much more massive machinery than the machinery that runs networks. A great example can be found in the analysis of the EINSTEIN project [11]. The EINSTEIN project was a piece of US government research to see how agency-wide or multi-agency-wide IDS-based (Intrusion Detection System) monitoring could be implemented. The idea of an IDS is that it inspects network traffic and tries to seek for anomalies or known signatures (of, for example, malware). IDS is therefore just a passive snooper in the networks. "The purpose of the 2004 EINSTEIN was to do real-time, or near real-time automatic collection, correlation, and analysis of computer intrusion information. IDSs were to be located at federal agency access points to the Internet."[11, p. 30]. The study quickly reached the conclusion that monitoring all traffic is a must if the goal is to detect all anomalies in the traffic. In other words, if one monitors only some of the network traffic, then it would be reasonable to deduce that some anomalous traffic would get through undetected. However, monitoring is very labor-intensive. It consumes resources beyond a reasonable cost. It was discovered that wide-scale IDS-based monitoring would be extremely labor-intensive, unscalable, and would create new security problems. If deployed, it would, indeed, be paradoxical.

Security hardware and software are certainly not flawless and can in fact make a system more vulnerable. One critical vulnerability case known as Heartbleed provides a fine example. The discovery of a vulnerability in the OpenSSL library, which is used by cryptographic services for SSL/TLS, left hundreds of thousands of trusted secure web servers open for an attack. The vulnerability received headlines globally, causing some panic over the Internet being "broken" [12]. The fact that makes the case paradoxical is that the Heartbleed vulnerability resides at the heart of information security itself. But how serious is it? Let us consider the fact, to begin with, that it allowed the leakage of primary keys, which are the "crown jewels" of security; with primary keys, it is possible to decrypt all messages captured. Anything that was once encrypted can be read in plaintext. The implementation of this cryptography had taken a great deal of work to deploy; it uses resources and it gives an impression of privacy and safety in its methods of altering the text into apparent gibberish. We trust these methods, and are usually more worried about vulnerabilities in other types of software – applications, etc. Yet it was the very core that was vulnerable, and the seriousness of this was amplified by

the fact that the vulnerability had existed for such a long time; it could have been used at any point over the whole time that it remained undetected.

Conclusion

Paradoxically, information security hardware and software increase the complexity of a system and in fact interrupt the system and users that information security is supposed to protect. As the systems are initially complex enough, information security can actually make the system so complicated that no one can control it perfectly. Counterintuitively, the tools of control make systems uncontrollable. The paradox is that although security measures increase complexity we cannot live without information security. The problem is that too much security cripples productivity, throughput, and steals valuable processing cycles. Thus, successful information security is about balance, how to achieve a required level of security without losing too much energy.

References

[1] T. Cook, "A Message to Our Customers," 16-Feb-2016. [Online]. Available: http://www.apple.com/customer-letter/. [Accessed: 15-Mar-2016].

[2] M. Castells, *The rise of the network society*, 2nd ed. Oxford ; Malden, Mass: Blackwell Publishers, 2000.

[3] M. Weiser, "Some computer science issues in ubiquitous computing," *Commun. ACM*, vol. 36, no. 7, pp. 75–84, 1993.

[4] T. Denning, T. Kohno, and H. M. Levy, "Computer Security and the Modern Home.," *Commun. ACM*, vol. 56, no. 1, pp. 94–103, 2013.

[5] A. Wright, "Hacking cars.," *Commun. ACM*, vol. 54, no. 11, pp. 18–19, Mar. 2011.

[6] J. Vuorinen and P. Tetri, "The Order Machine - The Ontology of Information Security," *J. Assoc. Inf. Syst.*, vol. 13, no. 9, pp. 695–713.

[7] J. Vuorinen, *Parasitic Order Machine. A Sociology and Ontology of Information Securing*. Annales Universitatis Turkuensis, 2014.

[8] S. Levy, *Hackers: heroes of the computer revolution*, 1st ed. Garden City, N.Y: Anchor Press/Doubleday, 1984.

[9] R. M. Stallman, *Free software, free society: selected essays*, 1st. ed. Boston: Free Software Foundation, 2002.

[10] K. P. Arnett and M. B. Schmidt, "Busting the ghost in the machine," *Commun. ACM*, vol. 48, no. 8, pp. 92–95, 2005.

[11] S. M. Bellovin, S. O. Bradner, W. Diffie, S. Landau, and J. Rexford, "As simple as possible---but not more so," *Commun. ACM*, vol. 54, no. 8, pp. 30–33, 2011.

[12] R. McMillan, "How Heartbleed Broke the Internet — And Why It Can Happen Again," 11-Apr-2014. [Online]. Available: http://www.wired.com/2014/04/heartbleedslesson/. [Accessed: 17-Mar-2016].

Jukka Vuorinen is a postdoctoral researcher in the Unit of Economic Sociology at the University of Turku, Finland. jukka.vuorinen@utu.fi

Pekka Tetri (pekka.tetri@gmail.com) is a Ph.D. student in the Oulu Secure Programming Group at the University of Oulu, Finland