Information technologies bring new and substantive threats to privacy - should they be curbed?

Marek Foss, 11/03/2008

1. Introduction

The rapid development of computer industry amazed everybody — both the IT experts, government, and society. This unexpected evolution of hardware, explosion of various software and growth of the Internet (in 2000-2007 between 100% and 900%, depending on region[1]), which emerged from a small university network, ARPANET[2], caught a lot of entities unprepared. Firstly, individuals not aware of the threats in malicious software and abilities not only **in** the Internet, but of **the** Internet itself (i.e. automated data extraction). Secondly, governments not ready for the legislation and social issues that rise because of this evolution. Finally, the IT professionals in the middle trying to keep up with the industry, i.e. grasp the constantly evolving organism the Web has become.

This paper will present the technology threats against society, especially in the field of privacy of individuals and groups. Also, it will try to answer the question whether it is necessary to take up any countermeasures and impose limits on this new technology by analyzing some of the consequences of the relatively high freedom that exists in the software industry and internet.

2. Privacy Definition

Privacy can have different definitions, and can be difficult to define, but one can intuitively know when his or her privacy is breached. The most frequently quoted on this matter is Introna[4], who categorizes privacy as a combination of three concepts: "limitation in access to personal realm, [...] control of personal information [and] freedom from judgement or scrutiny by others"[3]. It does not only mean individuals, but also privacy of groups.

Privacy issues are these issues that describe elements acting negatively on privacy like redefinition, limitation, threatening or complete elimination of privacy.

3. Threats Overview

Threats can be divided by different methodologies, but for the purpose of this paper we will use a following classification:

• hardware threats, i.e. monitoring devices like CCTV, hidden cameras, microphones, sensors etc.,

• software threats, i.e. malicious programs like viruses, trojans, spyware and other that can reveal sensitive data, purposefully or not,

• web threats, i.e. tracking, data mining, data analysis, database leaks, phishing and cracking (the last two can also be included in the software threats).

Threats imposed by the hardware are mostly created by the governing bodies, like governments, companies or administrators in order to rise surveillance and control over groups of people, often with a claim to increase security (although for example research on CCTV gives both positive[3] and negative[4] feedback). So far the threats were limited to identification of individuals in public places. Monitoring could be used to track a person's actions, recognize the person among crowd, store and analyze this data for various, even commercial uses. However, the monitoring was limited to public places and as such could not impose threats to individuals in personal spaces like homes.

But this approach changed with the recent proposal of US Department of Homeland Security (DHS) to implement Real ID[5] — a common ID card for US citizens, which besides various personal details would include a RFID[6] tracking chip. Strong opposition from the society not only brought the DHS to state that there is no will in implementing RFID (Real ID will use a barcode instead)[7] but to postpone the implementation deadline by years.

It is worth noting that with visible technology that the hardware is, the opposition in society is more likely to grow, and the control over the questionable issues of privacy lies in the society itself. And because only a limited number of bodies can implement a costly hardware technology, it is very likely this body has a lot of people watching over it, ensuring the opposition to any questionable actions is sufficient. As such, the hardware technology is easier to closely look after, curbed both by the society, and the media. And it should stay that way.

However it is exactly the opposite case with software and web threats. Common access to programming languages, freeware programming tools, and even ready made toolkits especially for malicious behavior make it fairly easy even for individuals to perform illegal activities on a large scale. In this case privacy issues are more serious than just surveillance — with correct software and web tools it is possible to obtain sensitive personal data, from embarrassing content or private photos stored on disk, to credit card details and security passwords.

Moreover, most of people do not realize how much data they give away each day on various websites. And with modern data crawlers it is possible to extract it and connect, to create a fairly interesting personal file with information recognized as private - from emails to phone numbers to family details, home addresses etc. All just from generally available data.

Therefore it is even worse when an actual data leak occurs. A fresh case is connected to Facebook social platform, where after an upgrade intended to tighten privacy settings [sic], a hack was discovered enabling viewing private photos, and among others, the celebrity Paris Hilton was affected[8]. More major cases include massive data leak of search histories by AOL (20M queries of 650K users)[9], or Government disks loss in UK with detailed personal data, including bank account identifiers of 25M citizens[10]. Significant is the fact that in the two latter cases the leaks occurred due to privacy policy breaches caused by employees, not by technology knowledge hacks. Countless attempts of phishing money account details or sniffing user activity through trojans[11] stopped hitting the headlines long time ago, but still exist and target the 'human factor' mainly, merely using the technology to hide its existence from the victim.

4. Conclusion

Summarizing, the freedom of the Internet and software development, vulnerable systems and procedures and finally even more vulnerable humans, create a dangerous environment for private data. Imposing limits and control is essential. The key thing is to distinguish responsibilities. The blame for this insecure environment is in humans, who firstly develop vulnerable systems, secondly exploit the vulnerabilities, thirdly are not willing to educate on safe system usage. Thus, the **limitation** should be imposed on humans, with correct and up to date legislation and enforcement units, while the **control** should be imposed on the systems, to monitor and catch possible vulnerabilities.

References:

[1] "Internet Users in the World, Growth Between 2000 and 2007", Internet World Stats (http://www.internetworldstats.com/images/world2007growth.png)

[2] "History of ARPANET", Antonio Cardoso Costa, Departamento de Engenharia Informatica (http://www.dei.isep.ipp.pt/~acc/docs/arpa-Contents.html)

[3] "The Illusion of Online Privacy", Barbara M. Wildemuth
(http://ils.unc.edu/~wildem/Publications/CHI2006-Privacy.pdf)

[4] "Privacy and the computer: Why we need privacy in the information society", L. Introna, Metaphilosophy
(http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp96/abstracts/introna.html)

[3] "Does Closed Circuit Television Prevent Crime? An Evaluation of the use of CCTV Surveillance Cameras in Airdrie Town Centre", Central Research Unit, The Scottish Office
(http://www.scotland.gov.uk/Publications/1998/12/978abe73-d412-4ea3-86a7-e5acf24c8d7a)

[4] "Police admit drunks not deterred by CCTV", Rosa Prince, Telegraph.co.uk
(http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/17/ncctv117.xml)

[5] "REAL ID", Department of Homeland Security
(http://www.dhs.gov/xprevprot/programs/gc_1200062053842.shtm)

[6] "Radio-frequency identification", Wikipedia.org
(http://en.wikipedia.org/wiki/RFID)

[7] "No RFID In Real ID", Emergent Chaos
(http://www.emergentchaos.com/archives/2007/03/no_rfid_in_realid.html)

[8] "Facebook security lapse allows Paris Hilton pictures to be leaked", Jonathan Richards, Times Online
(http://technology.timesonline.co.uk/tol/news/tech_and_web/article3617360.ece)

[9] "AOL Proudly Releases Massive Amounts of Private Data", Michael Arrington, TechCrunch
(http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/)

[10] "Data Leak in Britain Affects 25 Million", Eric Pfanner, The New York Times
(http://www.nytimes.com/2007/11/22/world/europe/22data.html)

[11] "Types of Scams", Bank Safe Online
(http://www.banksafeonline.org.uk/types_of_scams.html)