Securing the Internet: Fact or Fiction?

Basie von Solms

President: IFIP
University of Johannesburg
Johannesburg, South Africa
basievs@uj.ac.za

1 Introduction

The number of users of the Internet, in whatever way, is growing at an explosive rate. More and more companies are rolling out new applications based on the Internet, forcing more and more users to leverage these systems and therefore become Internet users. Social networking sites and applications are also growing at alarming rates, getting more and more users, whom we can call home or private users, involved and active on the Internet. Corporate companies are now also integrating social networking as part of their way of doing business, and governments are implementing Internet based systems ranging from medical applications to critical IT infrastructure protection.

Therefore millions of people are using the Internet for e-commerce, information retrieval, research, casual surfing and many other purposes, and this will just keep growing. One estimate is that the amount of data space needed to support the fast growing online economy will double every 11 hours by 2012 [1].

In most, if not all, of these activities on the Internet, data and information are involved. This may range from the user's IP address to secure personal information, to sensitive corporate information to crucial national strategic information.

The big question is, and has always been, how secure is all this information and data, and can it be properly secured?

This of course has worried experts even since information was stored in electronic systems many years ago, but has become much more acute the last few years with the explosive growth of the Internet, and the, in many cases, uncontrolled flocking of users to be part of Internet usage in some way or the other.

This paper objectively investigates this question, based on recent reports in the area of Information Security and Cyber Crime.

In paragraph 2 we will investigate what can we understand under the term "securing" of the Internet - what do we want to secure and why. In paragraph 3 we will give an overview of recent cyber crime statistics, and in Section 4 we will give an opinion about the possibility of securing the Internet.

2 What Do We Mean by "Securing" the Internet?

It is important to investigate what we have in mind when we say we want to secure the Internet, as there surely are different interpretations of this term. In this paragraph we will look at possible meanings of the term.

J. Camenisch, V. Kisimov, and M. Dubovitskaya (Eds.): iNetSec 2010, LNCS 6555, pp. 1–8, 2011.

2.1 The Ideal Interpretation

In the ideal and widest possible interpretation, we can say that securing the Internet means that all data and information stored on all websites forming part of the Internet, and all data and information being transported over the Internet are secured so that no unauthorized people can see (read) or change the content (protecting the confidentiality and integrity of the data and information), and that the data and information must be available to authorized users whenever they want to use it (protecting the availability of the data and information.)

This means that all information in all databases and in transit must be secured and only accessible to the authorized users. Apart from extensive encryption techniques to ensure this, extensive identification and authentication techniques must be available to ensure that every user is correctly identified and authenticated, and logical access control is comprehensively enforced. These measures must ensure that no person can masquerade as another person, and that electronic identities can only be successfully used by the real owners to which such identities were issued.

To create this ideal interpretation, the following must be possible:

- we must know precisely what is part of the Internet, ie which computers, servers and other equipment
- all these infrastructure must be controlled via legal systems to enforce the required confidentiality, integrity and availability
- no unauthorized system can be connected to the Internet - authorized by some (central?) managing power
- all users' identity information must be protected in such a way that it can never be compromised in any way
- all users must be absolutely aware of the risks of compromising their identity information
- legal systems must exist internationally which can enforce these requirements
- etc etc

Even a person with no information security knowledge at all, will agree straight forward that this ideal situation is NOT possible, because of the open and uncontrolled way the Internet is operated and growing.

Therefore, in the light of the ideal interpretation of securing the Internet, as discussed above, we must conclude

Securing the Internet is fiction - it is just not possible.

2.2 The Realistic Interpretation

Let us now investigate a more realistic interpretation. In this realistic interpretation, we have to accept that

- there is no, and never will be any, central control over the Internet
- there is no way to know what the boundaries of the Internet are, i.e. which systems are part of the Internet at any point of time

- no legal systems exist (presently) which can enforce any reasonable security (like enforcing encryption and proper identification and authentication)
- users do not protect their identity information, and are in most cases not aware of the risk of not doing so
- in no way can masquerading, or unauthorized use of identity information be prevented, as users are the weakest link in the chain and can always be seduced to compromise their identity information
- cyber crime is rampant and leveraging any possible chink in the armor of the Internet

Therefore, in the light of this realistic interpretation of securing the Internet as discussed above, the author concludes

Securing the Internet is fiction - it is just not possible.

This conclusion will be motivated in the next paragraphs.

3 An Overview of Recent Cyber Crime Statistics

An overview of recent cyber crime statistics, provides a good place on which to start and base a motivation for the view taken in the previous paragraph. In this paragraph, we will investigate some recent international reports on cyber crime, and try to get an impression of what is happening. The paragraph will be unstructured in the sense that we will provide a few quotes from specific reports, and then briefly comment on these in paragraph 4. Paragraph 5 will provide some suggestions for the future.

3.1 The Sophos Security Threat Report - 2009 ([2])

Under the summary, Six Months at a glance:

- 23 500 infected websites are discovered every day. That's one every 3.6 seconds - four times worse than the same period in 2008
- 15 new bogus anti-virus vendor websites are discovered every day. This number has tripled, up from average of 5 during 2008
- 89.7% of all business email is spam

The report further makes the following very worrying statement:

"The vast majority of infected websites are in fact legitimate sites that have been hacked to carry malicious code. Users visiting the websites may be infected by simply visiting affected websites, . . . The scope of these attacks cannot be underestimated, since all types of sites - from government departments and educational establishments to embassies and political parties . . . - have been targeted."

3.2 The CISCO White Paper ([3])

The White paper states that ***"Internet users are under attack. Organized criminals methodically and invisibly exploit vulnerabilities in websites and browsers and infect computers, stealing valuable information (login credentials, credit card numbers and intellectual property) and turning both corporate and consumer networks into unwilling participants in propagating spam and malware".***

An extremely worrying aspect reported is the fact that ***"trusted legitimate websites are the perfect vehicle for malware distribution. (it is estimated) that more than 79% of the websites hosting malicious code are legitimate websites that have been exploited".***

3.3 The UK Cybercrime Report 2009 ([4])

The report indicate that during 2008, ***"cyber criminals committed over 3.6 million criminal acts online (that is one every 10 seconds)". Furthermore, "online banking fraud has increased by a staggering 132%, with losses of UKP 52.5 million, compared to UKP 22.6 million in the previous year. This sharp rise can mostly be attributed to nearly 44 000 phising sites specifically targeting banks and building societies in the UK. Phising sites are becoming more prevalent and increasingly sophisticated."***

3.4 CISCO Annual Security Report 2009 ([5])

In this report, the following aspects are mentioned, which can let Internet users sleep uneasy at night!

"According to the Anti-Phising Working Group, the number of fake anti-virus programs grew by 585% from January to June 2009. Banking Trojans, like Zeus and Clampi, increased by nearly 200%".

An extremely worrying aspect highlighted in the report, is the growing use of mobile phones and text messages to lure the user into visiting infected websites. The report warns that this will have a huge impact on users as the use of mobile phones grows to gain access to the Internet.

"Expect to see more "smishing" scams (phishing attacks using SMSs) in 2010" warns the report.

Furthermore ***"as more individuals worldwide gain Internet access through mobile phones (because in many parts of the world it's faster to than waiting on available broadband), expect cyber crime techniques that have gone out of fashion to re-emerge in many developing countries. Cyber criminals will have millions of inexperienced users to dupe with unsophisticated or well-worn scamming techniques that more savvy users grew wise to (or fell victim to) ages ago."***

The report specifically refers to the use of other ways and approaches being used more and more for formal company work.

"Where does work happen? No longer does business take place solely behind network walls. The critical work of an organization is happening increasingly on social networks, on handheld devices, on Internet kiosks at airports and at local cafes. (This will) ***demand a new way of thinking about how to secure an enterprise . . . "***

3.5 T3.com ([6])

"There is now an epidemic of Malware online. Some experts are saying that there will come a point very soon where you can barely open a web page without coming under attack. . . . anything up to half a million computers could be falling victim to "drive-by downloads" each day. If you surf without any electronic safeguard, the chances are that you are already one of them".

In the same article, Mikko Hypponen from F-Secure is quoted as saying ***"However, even though we are not winning, we are certainly not giving up either."***

3.6 The Washington Post ([7])

"Law enforcement agencies worldwide are losing the battle against cyber crime. (the) number of compromised PCs used for blasting out spam and facilitating a host of online scams has quadrupled in the last quarter of 2008 alone, creating armies of spam "zombies" capable of flooding the Internet with more than 100 billion spam messages daily"

After this (sobering?) overview, let us now evaluate the situation in the next paragraph, returning to the author's view stated in paragraph 2.

4 Securing the Internet Is Fiction – It Is Just Not Possible

In this paragraph we will try to evaluate some of the aspects mentioned in the previous paragraph, and try to determine whether such aspects can be addressed in a way which can help to properly secure the Internet.

4.1 The Malicious Software (Malware) and Spoofing Threats

Can this threat be properly addressed? With legitimate web sites, for eg those of your favorite and trusted search engine, bank, sports club etc now being infected by malware, and your computer becoming infected by just visiting such a website, how will you know you are infected? Even if you have the latest antivirus (AV) software, the malware may not be recognized by the AV software, or the AV software may in itself be infected.

To a certain extent it can be expected that large corporate enterprises, having large security budgets, and a brand name to protect, may have advanced methods to detect such malware and protect their IT infrastructure, but it may not help! The newest type of malware may not be recognized by AV software, no matter how up to date they are. Such corporations still have to accept that their employees, logging onto the company IT infrastructure from unsafe sites, may cause infection - even if the strictest policies and procedures are in place.

However, the bigger worry should be about the home user, and even the small and medium enterprise who cannot afford to spend large amounts (even small amounts for that matter) on security of their systems, either because they cannot afford it, or they are not aware of the risks!!

How is this home user or small company user going to recognize a spoofed website? Even the security savvy experts have fallen for sites which are so well spoofed, that they just cannot be recognized as such? With 44 000 sites just concentrating their efforts on spoofing banking sites in the UK (see 3.3 above), the expertise and knowledge of those creating and operating these sites, must be such that the ordinary unsophisticated user will not recognize it!

Are users in developing countries going to be first put through awareness courses to sensitize them about potential risks and scams before they are granted mobile based Internet banking access, or are they just going to be left out there to fight for themselves (and lose their money?) (see 3.4 above).

It must take a very optimistic person (maybe with blinkers on), to state that all such users can, and will, be secure in venturing on the Internet.

The author's conclusion:

Trying to totally protect users in this environment is fiction.

4.2 The Threat of an Insufficient Legal Infrastructure for Curtailing Cyber Crime

Can we create and agree on a legal environment, accepted by all countries in the world, to ensure that all cyber criminals are caught and brought to book?

I am sure that even our very optimistic person of the previous paragraph, will agree that this is not possible!!

The author's conclusion:

To hope for a comprehensive, internationally agreed and cross border enforceable set of laws and penalties, to curtail cyber crime, is fiction.

4.3 The Threat of Error Prone Software Being Rolled Out

Many sites are infected by malware because of some error or flaw in the system software supporting user transactions - from the browser software through to the operating system software and other utilities. Such errors and flaws arise because of the immense complexity of these software systems - consisting of millions lines of code. These errors and flaws are then exploited by malware writers to infect

such systems. Patches are provided by the original suppliers when these errors become known, but some systems are never patched by their users, some errors are exploited before they can be patched, and some errors are exploited by the discoverer, and never reported!

Can such systems be developed, with the present level of software engineering knowledge, without such inherent flaws and errors? Can such systems always be patched in time before exploitation? Will all errors be discovered before exploitation?

The author's conclusion:

To hope for perfect software without flaws and errors is fiction.

5 Final Conclusion

From the discussion above, the author's conclusion is that presently, and with the present knowledge:

Securing the Internet is fiction.

6 So What About the Future?

Being negative about comprehensively securing the Internet and the users using the Internet, very definitely does not mean that the author is of the opinion that users should stop using the Internet - far from it! The positive side (benefits) of using the Internet, at least at this stage, still outweighs the negative side (disadvantages).

The Internet will only grow, and it will just keep serving more and more applications.

Any person who wants to buy a car, must have a driver's license. To obtain such a license, the person must complete a strict training course in which the potential driver is exposed to all the laws, rules, regulations and risks related to driving a car. If the user passes, and buys a car, he/she is doing that on an informed basis about the risks of driving a car, and the possibility of being injured or even killed in an accident. One thing you are never promised, and which every driver understands, is that there are NO promises by anyone that no mishaps will occur when driving. Driving without a license is an offense, in your own country and across borders.

The author's preferred solution lies in massive campaigns and controls to make users absolutely aware of the risks of using the Internet, so that they can take informed decisions whether they want to take the risk - they should know that they must take responsibility for their own security on the Internet, and should never think that someone else will protect them!

What must happen as far as Internet usage is concerned, and which must happen on a massive national and international scale, is that all users must be made aware of the risks of using the Internet. This will probably mean compulsory security awareness courses (with proof of understanding?) before a user

is granted Internet access rights. The user should be in a position to make a well informed decision of whether the benefits for which he/she wants to use the Internet, outweighs the risks. One thing users should never be promised, and which every Internet user should understand, is that there are NO promises by anyone that no mishaps will occur when accessing the Internet. Users should understand and accept that accessing the Internet has risks, and that it is not secure or safe.

We need an Information Security Internet Driver's License (ISIDL). Such a license should prepare and inform the user about the risks, related to potential financial fraud, loss of privacy, the protection of identity information etc, in accessing the Internet. Accessing the Internet without an ISIDL should be an offense, in your own country and across borders.

7 The End

- Accessing the Internet has many risks
- Securing the Internet is fiction and impossible
- Allowing users to access the Internet without such users being totally aware of relevant risks, is unethical, and should be prohibited
- Comprehensive national campaigns to inform users of the risks of Internet usage (to be run by Governments, introduced into schools etc)
- Comprehensive User Internet Security Awareness should be the entrance requirement before access is granted.

References

1. ITNow (January 2010), http://www.bcs.org
2. Sophos, The Sophos Security Threat Report (2009), http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threat-report-jan-2009-na.pdf
3. CISCO, A Comprehensive Proactive Approach to Web based Threats, CISCO IronPort Web Reputation White Paper (2009), http://www.ironport.com/pdf/ironport_web_reputation_whitepaper.pdf
4. UK Cybercrime, The UK Cybercrime Report (2009), http://www.garlik.com/press.php?id=613-GRLK_PRD
5. CISCO Annual Security Report (2009), http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf
6. T3.com (September 2009), http://www.T3.com
7. Washington Post, Cybercrime is winning the battle over Cyberlaw (2008), http://voices.washingtonpost.com/securityfix/2008/12/report_cybercrime_is_winning_t.html (accessed February 15, 2010)