# Security risks and patches – the effects of IT-vulnerabilities on the society

ATTILA HORVÁTH PHD
Foundation for Information Society, Senior researcher, consultant
horvath.attila@infota.org

***ABSTRACT***

The following paper contains a small part of a three years study on the effects of software vulnerabilities on the economy and the society, with the support of Hungarian Scientific Research Fund (project number: PD-109740). This paper summarizes the basic examination methodology of IT-vulnerabilities, the research environment and the basic end-user effects based on a sample basket of the most commonly used client software products. Finally it defines trust within the ICT environment, and summarizes the most important solutions for keeping up trust in this more and more dangerous environment.

# Introduction

The Infocommunication Technologies (ICT) is more and more affecting our lives. The application of these technology drivers covers both the homes and the economy. We take their presence as granted. They are parts of the everyday infrastructural services. Therefore their deficiency or absence can so severely affect the economic role-players or households as the missing of any other critical infrastructural resources. If we add to this that these technologies include and preserve nearly the whole information wealth whether it is official or governmental data or family photo album, we can see that their perfect secure operation to be maintained can be considered as a public interest.

The permanently traceable digital convergence, i.e. the information and data handling, communicational value producing, moreover entertaining and other functions are concentrating in to less and less devices that is increasing the operational failure risks of the systems. The less number of devices used for the necessary functions, the more critical their optional failure will be.

The problems, deficiencies of these areas are primarily approached the technological side, although the system failure deficiency or even willingly carried out attack can have a strong spill-over effects in the economy and the society.

These deficiencies can cause great harms, and we could say that their avoidance is basically a technology or IT task. This can be considered true, but we cannot ignore some serious complementing circumstances. For the measurement of these effects practically there is no unified methodology it would be important to be able to express them in a quantified form.

On the one hand a methodology is needed for the technological investments and the funding of protection measures, as neither on governmental nor on company level generally the experts making decisions the frame numbers have an IT-degree, thus it is exceptionally important that we make the problems understandable for them. On the other hand the general social confidence towards ICT has been decreasing by the inappropriate problem handling, which endangers the strategies aiming at modernization and digital literacy.

A three year research concerning the effects of IT and network vulnerabilities on economy and society has begun in 2013 which is implemented by the author in ligament with the Foundation for Information Society with the correspondence of the National Cybersecurity Center and the support of Hungarian Scientific Research Fund (project number: PD-109740).

The aim of the project is that the data obtained during existing and future cooperation carried out with CERT, should be compared to the secondary data sources reflecting the IT-knowledge of the national economy. In the framework of the primer research the project would assess the real effects of IT-vulnerability in the operation of the economic and public role-players and thus it would evaluate the effects that could be caused by the resulting risks and their inappropriate handling in the economic performance.

The first research objective is to examine the topic at an end-user level. Taking into consideration that the current hardware and software tools of the population as well as their IT-knowledge and readiness, the research attempts to find an answer how these IT-risks can influence the lives of the users related to availability and functionality of the tools and systems used by them.

# 1. A World connected as never before

In this digital era we can speak about a hyper-connected society. Just Google reported over 500 million new android activations per year and 40% percent of the globes total (over 7 billion) population is connected to the internet.

Internet users, according to the United Nations International Telecommunications Union (ITU, 2014), are expected to hit 3 billion by the end of 2014, which accounts for about 40 per cent of the world's population. Among those users, over three quarters are from developed countries while two-thirds come from the developing world. Moreover, people from developing countries make up for more than 90 per cent of those who are not yet using the Internet. For further details see Figure 1.

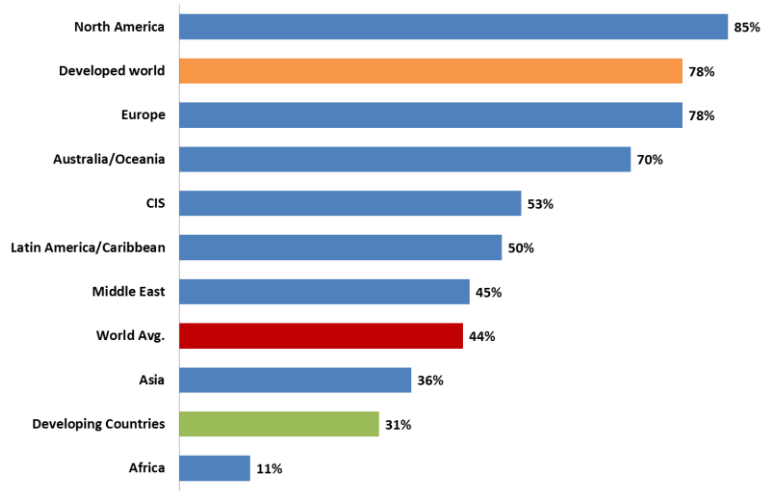


Figure 1: World internet penetration in 2014 (Source: ITU, 2014)

In Africa, about one-fifth of the population will have access to the Internet; while in the Americas, nearly two-thirds of the population will be online by the end of the year. Further, Europe has the highest Internet penetration rate of 75 per cent, while the Asia-Pacific region has the largest population of Internet users.

Turning to mobile-broadband penetration, the number of its subscriptions will achieve 2.3 billion globally. 55 per cent of them are expected to be in the developing world. As shown in the ITU statistics, mo-

bile-broadband remains the fastest growing market segment, with continuous double-digit growth rates in 2014. In addition, Africa takes the lead in its growth, from 2 percent in 2010 to almost 20 percent in 2014.

## 2. The burdens of cyber-attacks

Cybercrime is a growth industry. The returns are great, and the risks are low. According to experts estimate (CSIS-McAfee, 2014) the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest of these figures is more than the national income of most countries and governments and companies underestimate how much risk they face and how far the spillover effects go not only in the corporate or the government sector but in the world of end users and the whole society.

Deciding what counts as cybercrime affects the size of any estimate. Most estimates contain both direct and indirect costs, and data used that takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked company. These additional indirect costs show the full effect of cybercrime on the global economy. International agreement on a standard definition of cybercrime would improve the ability to collect consistent data.

Even a broad definition leaves out important nonmonetary effects on innovation, common trust in ICT, digital literacy, national defense, and the long-term competitiveness of societies, countries or companies.

Most incidents go unreported. Few companies come forward with information on losses. When Google was hacked in 2010, another 34 Fortune 500 companies in sectors as diverse as information technology and chemicals also lost intellectual property. (Cha-Nakashima, 2010) Some of the information on the incident only came to light from documents made public by WikiLeaks. Only one other company reported that it had been hacked along with Google, and it supplied no details on the effect. Similarly, when a major US bank lost several million dollars in a cyber-incident it publicly denied any loss, even when law enforcement and intelligence officials confirmed it in private.

The lack of data means that any dollar amount for the global cost of cybercrime is an estimate based on incomplete data. A few nations have made serious efforts to calculate their losses from cybercrime (mainly in the developed world), but most have not. Most studies assume that the cost of cybercrime is a constant share of national income, adjusted for levels of development. The calculations are based on the likely global cost by looking at publicly available data from individual countries, buttressed by interviews with government officials and experts.

High-income countries lost more as a percent of GDP, perhaps as much as 0.9% on average. This may simply reflect better accounting, but rampant underreporting means that actual losses may be higher. For developing economies where IP plays a smaller economic role, the losses averaged 0.2% of GDP. The average loss among all countries for which we found data was 0.5% of GDP.

The data quality on losses is very heterogeneous. Certain resources assume for example that losses in the EU totaled only $16 billion, far less than anyone would estimate, while others speak about almost a trillion dollars. (CSIS-McAfee, 2014) Under such circumstances it is very difficult to give any well-established calculations. The problem is even worse in the developing world, where most governments do not collect any data on incidents and losses at all.

# 3. Broken shields: Software vulnerabilities

What's a security vulnerability? Most people think this would be an easy question to answer, but in fact it turns out not to be.

For the context used in the software security industry, vulnerability is a security exposure that results from a product weakness that the product developer did not intend to introduce and should fix once it is discovered.

A security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.

A software vulnerability can be seen as a flaw, weakness or even an error in the system that can be exploited by an attacker in order to alter the normal behavior of the system. Because the number of software systems increases everyday also the number of vulnerabilities. Additionally, if we consider that most of the systems are exposed to multiple users (internet) and environments (operating systems for example) then it is just a matter of time that someone can launch an attack (sequence of actions) whose consequences are unpredictable in damages and cost. Usually the goal of an attacker is to gain some privileges in the system to take control of it or to obtain valuable information for its own benefit. Then it is important for the developers and general public to know about vulnerabilities and their prevention and detection.

These vulnerabilities are present in the commonly used consumer and business software products form operation systems to browsers, from document management software to video/music players, making it possible for potential attacker to access.

# 4. Vulnerability research

In this part of the research contains an attempt to establish a methodology for the stochastic risk analysis of computer terminals (clients) knowing that the time series of these events are generally not available, in many cases not even the entire event space is unable to be obtained. To reach our goals we developed a model to analyze the security risks of IT systems based on the three known risk analysis methodology (quantitative, qualitative, stochastic). In this model the examinations are based on real-life vulnerability data, and the desired outcome is to identify how certain IT environments are affected by the vulnerabilities on the accessible vulnerability lists.

The basic phenomenon here is the probability of occurance. The expected value can be defined as the product of the damage caused and the perceived probability of occurrence, in case both values are known or can be calculated.

The probability of occurance – based on the definition of BME Security Management Research Group (SMRG, 2003) – is the likelihood that an event (incident) - the threat based on the identified vulnerability – is realized in the form of an attack.

There are multiple methodologies to calculate the effective damage:

- The difference between the first total value of the residual value (loss of tangible value)
- Re-production value (new value)
- The costs of the elimination of the outcomes (recovery value)
- The damage of intangible assets (loss of intangible value) (goodwill, consumer trust, etc.)

Most threats affect certain IT applications, database management tools, operating systems, so the first task is to properly define the baseline "IT environment" on which the further investigations are carried out. All software elements used for the IT activity of the chosen target group - applications, middleware, database management systems, operating systems, plug-in software, firmware, etc. – are part of this system. In the further investigations these elements are arranged in defined IT_ENVi sets like end-user, smartphone, corporate clients, government clients, etc.. These groups are defined by choosing a certain mix of compulsory elements of the environment - such as an operating system - and optional elements - such as middleware. Now the certain IT_ENVi environments and threats can be associated.

To determine the involvement of the certain IT_ENVi environments in the system above, a database has been built first from the vulnerability data of PTA CERT-Hungary National Cybersecurity Center (2010.01-2013.06), then - after the central restructuring of CERT-Hungary in the last year - directly from the US-CERT event database (2013.07-).

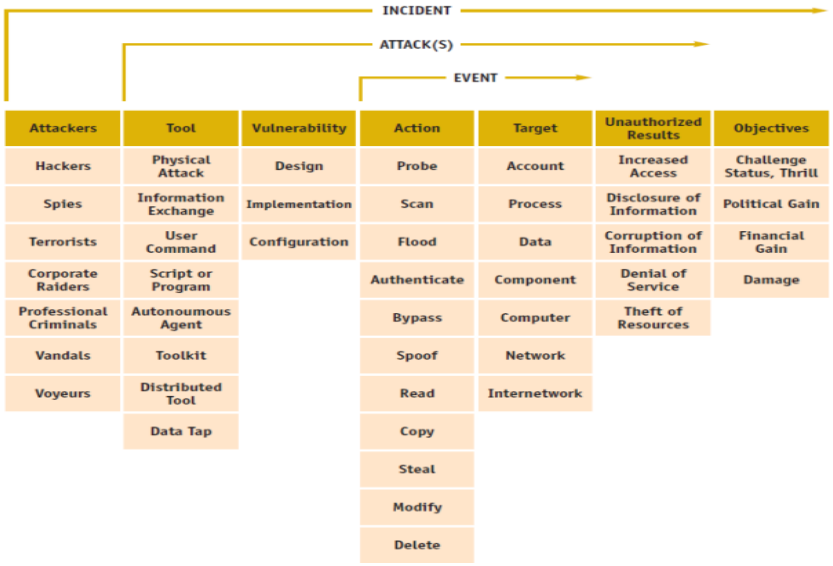


Figure 2: CERT - Common Language Security Incident Taxonomy (ENISA, 2014)

The structure of the database is based on the SANDIA classification system from 1998, which is the predecessor of the official taxonomy used by CERT under the name of Common Language Security Incident Taxonomy. (See Fig. 2.)

The database content is based on a complex research and data collection work within several independent resources:

- The National Vulnerability Database operated by US-Cert (USA Homeland Security)
  - As the main software vendors and software vulnerabilities and are international, this resource is appropriate to fulfill the research needs on any market.
- The vulnerability database of Secunia Advisories
- Mitre.org – Common Weakness Enumeration (CWE)
- Vendor reactions and data (based on internet search)

# 5. Connecting vulnerability data to the end-user environment

To assess how exposed endpoints are, the types of products typically found on an endpoint are analyzed. Security software vendors like Secunia, Kaspersky, F-Secure, Symantec and Sophos are gathering anonymous data from scans of the millions of private computers which have their protection software installed. The computer of a typical end-user has an average of 75 programs installed on it. Naturally, there are country- and region-based variations regarding which programs are installed. Therefore, for the sake of clarity, a representative portfolio of the 50 most common products found on a typical computer has been assembled and the most used operating system has been identified. These 50 programs are comprised of 33 Microsoft programs and 17 non-Microsoft (third-party) programs.

The most commonly used OS in the previous year has been the Windows 7, although Windows XP, Vista, and Win8 are also gain a measurable market share. The number of vulnerabilities discovered in these products has been, 102 for 7, 99 for XP, 102 for Vista, and 156 for 8. The high number of vulnerabilities in Windows 8 is due to the fact that Windows 8 has Adobe Flash Player integrated into Internet Explorer. This integration is responsible for a high portion of the vulnerabilities (55) detected in that operating system.

The Microsoft part of the sample contain software products like Internet Explorer, .NET, Office products, Silverlight, XML Services, Media player, Defender etc.

The top 3rd party products within the sample are Mozilla Firefox, Google Chrome, Oracle Java, Adobe Reader/FlashPlayer/Air/Shockwave, Apple iTunes/Quicktime, VLC Player, Skype, etc.

These software products are commonly present on end-user computers, and they are heavily defining user experience and common trust towards ICT.

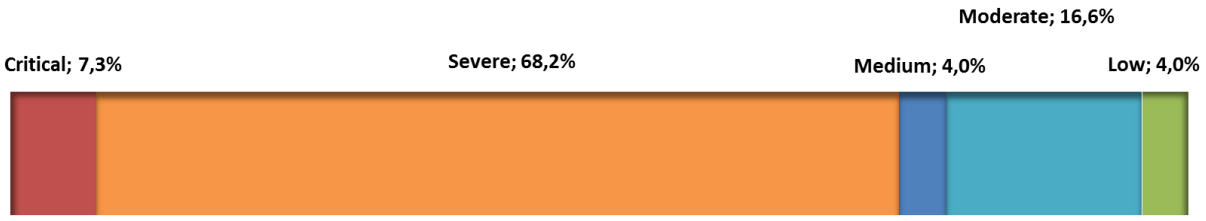


Figure 3: The distribution of vulnerability severity within the end-user sample 2014.

Figure 3. above represents the severity of the certain vulnerabilities. Severity is levels are based on the damage potential of a successful exploit. It raises the probability and danger of successful attacks that 87% of the vulnerabilities above can be exploited through a remote network access. In case of end-user group it is highly improbable, that a potential attacker accesses the local network (except for hacking a WIFI from the street) or gaining direct local access to the computer. To do this a physical break-in is needed to the users home, which is more difficult to realize than creeping into an office building.

The common solution for discovered vulnerabilities are patches. Vendors try to correct the errors as soon as possible in most cases. In case of the most commonly used end-user programs, the vendors affected are multinational players who usually provide solution within one day from discovery.

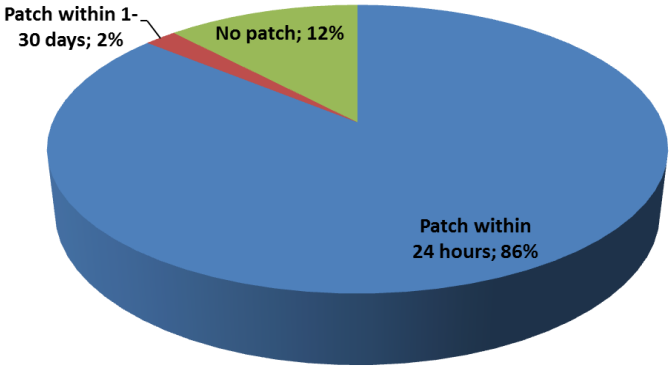


Figure 4: Patch availability within the end-user sample 2014.

In certain cases the vulnerability affects a structural part of the software product, where it is much more difficult to solve the problems. That is why the patches are delayed in 2% percent of the cases, or there is no patch at all. In these cases usually there is an alternate solution: for example switching out or avoiding certain functions until the new main version is released where the error is corrected. Of course in case of discontinued products, like WinXP, or IE6 it can happen that no solution is arriving. In these cases the only possibilities are the tricks above or changing to a supported generation of the software.

The most dangerous scenario is that an attacker can exploit a vulnerability before it is discovered by the vendor/IT community, so that developers have not had time to address and patch. This is called a zero-day attack, because the programmer has had zero days to fix the flaw. Luckily zero-days are quite rare. In the last year from the total 1208 vulnerabilities only 10 has proven to be zero-days, so the exploit begun before preparing a proper solution.

# 6. Effects on trust

New technology is a central part of economic development. However, transformation in economic possibilities through new technology often creates social tensions and new questions in paralle1. Unless we recognize and address the social challenges related to digital information, there is a risk that opportunities to use it are missed.

Trust in an important feature which underpins the use and value of new technologies and therefore can support the development of a digital economy. Businesses can build trust at an individual level by implementing good practices. However, good practices need to be underpinned by clear social expectations and legal obligations. We identify four essential elements to building broader trust around digital information.

To be very harsh there is a huge gap between the way the current security solutions and the requirements of the normal end user.

The common user has these requirements:

1. Don't think, just click.
    - Users don't want to be bothered with anything that stands in the way of what they want to do. It won't work.
2. Someone else must protect me.
    - Users assume that their computer keeps them safe from all harm. Or their virus scanner. Or their ISP, or faceboogle, or their government. But at the same time, these appointed

chaperones must respect their privacy.

3. For free.
    - Of course, users don't want to pay for anything.

One might call it unfair of these users, however, mostly they are not to blame. It's what has been promised time after time, albeit never delivered.

Trust is binary. When people use a technology, install an app, visit the web, either they trust it sufficiently to give identifying details, or they don't and refrain from using that thing.

Trust decisions can change at any time. It can be friends, family, the local IT guy or the ISP who is able to change a user's trust decision. Or it can be an error on the screen to spark distrust. It can be a learned behavior as well: "There is this green bar, so it is OK." There is no rational thought process behind it.

To minimize the negative effects at the end user side **one key point is the communication**. Communicating risks, possible outcomes, and the things needed to do is one way to preserve trust. For example to minimize the negative effects of a security breach transparency and communication is key, as clients are often more concerned with how an organization responds to a breach than the fact that it occurred. The reason for the mistrust mostly is not because a vendor ort a service got hacked. People know that people get hacked. The problem with the lack of proper communication is that people lose faith, that the target knows that happened and knows how to take care of it.

The second thing is to **make users to do their part of the job** within the restoration process: use and install the patches and/or new main versions. According to this research is case of the most commonly used end-user software product like browsers or pdf reader applications the proportion of unpatched products can reach 30-50%, because it is not a must for further usage.

The third solution is to **apply "no-brain" security measures** within these products: automatic patching and updates can be the answer, together with the impossibility of use of the compromised version.

# Acknowledgement

Preparation of this study is supported by "The effects of IT and network vulnerabilities on economy and society" no. PD-109740 from Hungarian Scientific Research Fund (OTKA).

# References

[1] Ariana Eunjung Cha and Ellen Nakishima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," The Washington Post, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

[2] Center for Strategic and International Studies (CSIC) – McAfee: Net Losses: Estimating the Global Cost of Cybercrime, June, 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[3] United Nations International Telecommunications Union: The World in 2014, ICT facts and figures, April, 2014. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

[4] Budapest University of Technology and Economics, Faculty of Economics and Social Sciences, Department of Information and Knowledge Management, Security Management Research Group (SMRG): The Glossary of IT Security Concepts p.4.

[5] European Union Agency for Network and Information Security (ENISA): Common Language security incident taxonomy, Sept, 2014, https://www.enisa.europa.eu/activities/cert/support/incident-management/files/figure11.png/image_view_fullscreen