An Overview of Cyber Insecurity and Malicious Uses of Cyberspace

Rui Miguel Silva[1(✉)] and Ivan Zelinka[2]

[1] Lab UbiNET – Computer Science Security and Cybercrime/LISP – Laboratory of Informatics, Systems and Parallelism, Superior and Management School, Polytechnic Institute of Beja, Rua Pedro Soares, s/n, 7800-295 Beja, Portugal
ruisilva@acm.org

[2] Department of Computer Science, Faculty of Electrical Engineering and Computer Science, VSB-TUO, 17. Listopadu 2172/15, 708 00 Ostrava-Poruba, Czech Republic

Abstract. Cyberspace entered in our lives for years, in all the domain areas of modern societies, since gamming and fun, from sport information to political and cultural news, scientific dissemination, governmental and public duty activities and all of these domains create a new economical and financial really. Nowadays "People and Money" are on cyberspace and these turns the focus of crime activities to cyberspace. By other side, cyberspace gives fast access from one corner of the world to other corners of the world just in a mouse click and all these with physical cover. So, cybercrime, and all the other "cybers", like cyber security, cyber defense, cyber warfare, cyber terrorism, cyber hacktivism, or cyber spy, came to stay in the real world. The talk will overview the state of the art of the bad uses or malicious uses of cyberspace due to insecurity and benefits form cyberspace as a platform for malicious activities.

Keywords: Cyber security · Hacking · Cybercrime · Cyber terrorism

1 Introduction

We live in a modern world where technologies surround us at every step. Smart phones containing the operating system that wakes you in the morning, show the latest news and weather forecast. On the way to work you perceive technology, which is packed in your car. In your job, you have to choose - do the hard work or use technology and spend time in front of computer screen. One simply cannot imagine life in the 21st century without technology.

The modern age is heading more and more towards globalization and mutual connectivity. There are other connectivity options - it is a common practice to have your phone incessantly connected to the network of mobile operator and use data connectivity. Also, wireless connection is present in buildings, you can connect with public transportation and soon in aircraft. Time still goes by, new and new devices connect every day to the world wide web - from computers, tablets, phones, TVs to watches, glasses and other wearable devices. In upcoming years your homes, cars, washing machines, blenders, cutlery will be connected … eventually even yourself.

V.H. Duy et al. (eds.), *AETA 2017 - Recent Advances in Electrical Engineering and Related Sciences: Theory and Application*, Lecture Notes in Electrical Engineering 465,
https://doi.org/10.1007/978-3-319-69814-4_2

All the positive aspects have a dark side. Analysis of all the possible negatives would need its separate philosophical work. The reader will, therefore, be introduced to one important and very extensive topic that the technology development opens - computer security and especially malicious code (also known as malware). Every individual is imperfect, and that is also reflected in technologies such as computer systems. The more the world connects and systems become more extensive, the more options offenders acquire. Note that malicious codes are not directed only at the computer itself, but also at other electronic devices that may be open to attack. The reader should be aware that such devices may interfere with his private life and contain personal or valuable data. Including the computer banking systems that manage your finances.

It is obvious that unauthorized manipulation with such systems can damage individuals, groups, institutions and whole countries on a global scale. You will feel the consequences significantly more if you happen to be the offender's victim and if the attack is successful. These initiatives prompted me to further thinking: "How easily can an attack become successful? How can I be attacked in the digital world and what may be real consequences? Are the systems protected as much as possible to eliminate the risk?".

These questions provoked my interest in this issue. During the project, I, therefore, try to impersonate the role of the attacker, so I can better understand the tactics of the offender and to use the knowledge for better prevention and detection of attacks. I further use the knowledge to improve the security of systems I manage and programs I have created. Theoretical and practical information is also shared with those who want to participate in increasing the security of computer systems.

Information play at today's communities crucial role. In initial period expanding computer technology in last decenniums head spending on acquisition, what biggest availability as well as connectivity computing system. On safeguard mostly anybody too didn't seek, since its consequential application in the unshot, IT solving is getting more expensive and stunning first nominative aims. At the turn of the millennium but got thanks, immense number and miscellaneous computer attacks and considerable damages with them connected to realize sobering up and to the forefront now are given above all protection of information reside in computers. Thanks that today keep at one's disposal reliable antiviral agent, firewall, systems detection penetration, Windows update, antispyware, spamming filters, advanced version operating system and next technology, that we save. They will look at such development at all behind several years security specialists need. According to the opinion fore world's security experts and according to our daily experience four - square yes. Safeness though is given without comparing more attention than in former times, as well but shoot up to the number and complication technology, that be necessary at protection impeach. Today though already passed away time naive attacks, when 15 - year - old hacker was able to trigger squeeze struck scripts take sb. Down a peg or two biggest web servers on the internet (case Mafiaboy, the year 2000), certain of nevertheless cannot be truly an anybody. As well as improved, our defense namely advanced and technology and routes ambushers. Mentioned instances some incidents from the year 2008:

- Error in system DNS detected Danem Kaminskim that they make use of so - called birthday paradox hereto, to proof forge communication with DNS server and corrupt his cache threatened whole infrastructure internet by that the ambushers allow redirecting any web and email servers. Only thanks, extra charges cooperation by many interesting subjects all the world over (manufacturers DNS servers, operators, ISP, …) were to be affected steps to the elimination of mistake before her publication abroad. Weather was an error detected and misappropriated even before her retrieval Danem Kaminski is not known.
- First malware penetrated already also into cosmos – worm W32. Gammima. AG was captured on international space station IIS in notebook one of Russian astronauts.
- A few years ago on conference BlackHat was attention concentrated on possibility development universal rootkitů for router Cisco. Routers those brands other about roughly 2/3 Internet running if development such rootkits succeed they hackers may obtain an enormous power.
- In France cowboy stole money out of bank account president Nicolas Sarkozy did not act at the same time about no organized group high - level but about two small money cheats. Isn't then too gutsy speculate that the against goal - directed cyberútoku able attacker would be immune hardly anybody.
- In Chile exposed unknown cowboy stole and published in the internet name and description six million Chilean citizens.
- Security slip - up was detected in the system new Boin 787, mine traveler approach from his utilities into nets destined for flight instruments. This sure doesn't need next comment.
- Obviously, the chief modern mobile telephone is vulnerable in the face of attacks by the help of Bluetooth or MMS. For example near some version popular Motorola RAZR to installation harmful software be enough only receive MMS with infected JPEG file. Such apparatus it is possible then change for example in bug cause - sending all talks and text news In future also most probably wait to see botnet formed by mobile telephone.
- Security mistakes were to be detected in coffee machine brands Jura F90 (electric coffee percolator has reticular interface enabling set at a distance). By itself it sounds almost funny, nevertheless successful abuse this error can lead as far as to compromise PCs. with Windows XP connection with an electric coffee percolator. Presently rather is concerned interesting rarity, but isn't far way off time, when almost any electronic set up in consumer sector including electrical wall socket will have it's own IPv6 address (draft so - called intelligent home). The impugnable surface then again will overgrow.
- On October 2008 was once again detected an error in RPC system intercurrent all presently supported version operating system Windows (2000, XP, 2003, Vista, 2008). By the help of mistakes, it is possible on the remote system to start any code underneath system account (i.e., in the worst case for install rootkit). Slip - up is in so far relevant that the Microsoft quite exceedingly published patch out of the common term issue stale mate (every other Tuesday in a month). This time had Microsoft luck because error discovered before the adverse party, otherwise would with biggest probability wait to see similar worm what was the famous W32. Blaster in the year 2003.

Apparently, computer attacks certainly don't fade away and imagination their authors rather year after year shoot up. What more – according to eminent antivirus companies Mcafee's roughly since 2007 culture Internet nether world very much switched at that sense that the disappeared young hackers (so - called script- kiddies), who create viruses and hacker PCs. Simply for laughs and out of curiosity and replaced is organized gangs, professional offender. Today in this area largely is concerned money Arose all gray economy, in which it is possible services hackers, makers spyware, and demise bot - that purchase is like any other product.

Threats then growth as well as have to grow our knowledge, so that to these menaces prove successfully stand. In the battle against any antagonist, it is necessary to know his friend – his game, acquirements, tools, and motives. Activities, knowledge, and skills that serve for this purpose usually called ethical hacking, people whom he does then "whig-hat" hacker. It is impossible to deny that the information desk, that is in those and similar publications at the disposal it is possible in the same way anyhow to prevent abuse to transaction computer attacks. It is only unavoidable aspect education and solving certainly isn't such information desk bottle up and censor – adverse party towards them in the same way she will get because despite gigantic variety motives and intentions all hacks link curiosity and longing getting to know.

Company and individuals have to know, how to computer damages happens. What are the genesis of computer attacks to better be prepared and awareness to face it. We believe that there are two key aspects that lead to computer attacks, first the Cyber Insecurity and second the Malicious uses of Cyberspace.

2 Cyber Insecurity

The first issue that leads to cyber insecurity is the access to information. It's possible and very easy today, for anyone with access to Internet, to get information of an individual or a company. With that information it may be possible, and in most cases its really possible, to identify weaknesses and vulnerabilities, even technical or human, that allows a better plan for a successful attack. Sometimes the information is just there accessible to anyone, other times co-relation of the information gathered, with or even without Intelligence technics and tools, leads to those information that helps on attack plan. The information gathering process uses two kinds of procedures, resources on the Internet, and specialized tools developed specifically to gather some particular kind of information. Some examples of resources on the Internet are: (i) simple Google search or other search engines; (ii) statistical collection sites like "www.alexa.org"; (iii) the Internet archive which stores every page that appears on the Internet at "www.archive.org"; (iv) black lists that of web or emails servers for instance, like "www.dnsbl.info"; (v) or information about the operating system and the web server software of a target site, like in "www.netcraft.com". Examples of specialized tools for information gathering are: (i) "DNSENUM" available at "github.com/fwaeytens/dnsenum", which uses the Domain Name System to gather several information for a target, such as "nameservers", "MX record", or "reverse lookups on netranges"; (ii) "WHOIS" available in several flavors that gives information about the registered domains including technical and management stuff of a target company; (iii) "theHarvester"

available at "github.com/laramies/theHarvester" which gathers information such as "email accounts", "subdomain names", "employee names" or "virtual host names"; (iv) "Metagoofil" available at "github.com/laramies/metagoofil" that extracts metadata of public documents like PFDs, DOCs among others, that are available for a target website, and from this information it could be possible to get "usernames", "personal names", "paths in the computer system" where the documents was generated, and all this could be useful for a better planning of attacks; (v) or, last but not really the least, "NAMP" available at "github.com/nmap/nmap" which allows, among other things, the identification, or at least a very good guessing, of the "operating system", "the open ports" and "software running on that ports", for a target computer system.

Besides information gathering easily and open access, the huge spread of Internet access flavors available from Telecom companies, which hardly fight for bigger quotas of clients that uses them as Internet Service Providers, has dramatically spread Internet access to many houses in the so called "developed societies". Most of the common clients use to subscribe the, also so called, "Packet Services" which includes, TV, Phone, and Internet, and in some cases, also Mobile Phones and even High Band Internet Mobile Accesses. Using this "Packet Services", many users have a permanent Internet connection at their homes. Sometimes, if not in most cases, with no security measures as anti-virus or firewalls. Besides that, we truly believe that many users, try to get free contents from piracy sources on the Internet, such as music, movies, technical books, among others, using for instance peer-to-peer-file-sharing protocols and platforms like BitTorrent. This process could lead to the exploitation of vulnerabilities on the cyberspace users computer, such as backdoors that allow hackers to take control on the infected computer. Other common activity among cyberspace users is the use of search engines to get free players or file readers, such as "AVI", "MPEG3" or "MPEG4" players, or "PDF" reader. A simple search with three words "free", "download" and "reader", on Google gives 27 700 000 results. The trustiness of the download sites is not questionable, for the common cyberspace user, which simple click on, download the software and install it on its computer. This behavior comes from a yet very weak cyber culture, where cyber security is not yet on its right place of concern. But at the same time may users, use them computers to access Home Banking or submit personal financial data to E-Government platforms. This lack of cyber education, which would provide cyberspace users with the knowledge and conscientiousness of cyberspace risks, is the most important component of the cyber insecurity.

As was implicit in the Introduction of this paper, software will always have vulnerabilities, even due to the complexity of software integration which imports libraries and software modules that was not correctly validated, or due to insufficient care on security aspects form programmers, or due to "not so good" program skills or many other aspects, we should always count with software vulnerabilities. But besides software vulnerabilities, there are also the default or weak configurations. This aspect is sometimes used by hackers to achieve successful attacks, instead of software vulnerabilities. For instance configuration of systems with username "admin" and no password defined, or systems with username equal to the first name of the user, and weak passwords like "12345678". These caricature situations are not so uncommon. Stepping a little bit in the weak configurations world, some system administrators keep the Well Known Ports on common services, such as SSH access on port 22, leading to

brute force attacks on them systems, using applications like Hydra to automate the attack for instance, which then, simple needs to have a "stupid" user with a weak password, to compromise the all system. On another perspective of weak configurations we face the fact of many Internet Service Providers installation teams that leave the default usernames and passwords configured on clients Router and that way, exposing them clients to easy attacks. This incredible and un-responsible behavior is faced in many real word cases.

Software vulnerabilities and weak configurations are publicly announced and there are normalized notations for it. Software vulnerabilities are normalized in Common Vulnerabilities and Exposures (CVE) accessible at "cve.mitre.org/" and weak configurations are normalized in Common Configuration Enumeration (CCE) accessible at "nvd.nist.gov/cce/index.cfm". These two notations are part of a bigger set of languages, notations, and classification systems, promoted by MITRE and NIST and other organizations, as a way to manage cyber security. However, at the same time these publicly announcements of vulnerabilities and weak configurations, could aware and help conscientious chief security officers (CSO), it also could helps those hackers who are waiting for these announcements to try to attack less conscientious CSOs. So, the same information could help good or malicious uses of cyberspace. In the next section we focus on "some" malicious uses of cyberspace.

3 Malicious Uses of Cyberspace

The existence of "Vulnerability repositories" like the National Vulnerability Database (NVD) at "nvd.nist.gov" allows and facilitates the search for known vulnerabilities. So, a normal way of thinking by an attacker should be, after a good information gathering about its target, search on vulnerability repositories for known vulnerabilities that he could explore on his target. But the knowledge of a vulnerability that could be explored, does not explore the vulnerability itself, it is needed an exploit that could take advantage of the vulnerability. Meanwhile a vulnerability indicates some kind of weakness on the software development that could be used to break the security of the software, an exploit is a concrete piece of software that effectively "exploits", that effectively "takes advantage of a vulnerability to exploit" the software. So an exploit is a practical weapon, not an hypothesis, not conceptual, nor even a theoretical way to explore. In this part of our journey comes the "Exploit repositories" like for instance Exploit Database at "www.exploit-db.com", which at the time of this writing has 37 771 exploits archived. So, if an hacker has a target to attack he could do this three steps procedure: (1) Information gathering; (2) Vulnerability repositories; (3) Exploit repositories.

However, sometimes, hackers do not have a specific target, they simple have the knowledge of some vulnerability and the respective exploit to use, so in this scenario, the hacker does not care about who is the target, or victim, he just wants to find someone vulnerable to the exploit he possesses. In these situations, cyberspace has also the answer; there are the "Dork repositories" like the "Google Hacking Database" (GHDB) at "www.exploit-db.com/google-hacking-database". Dorks are expressions that could be used in search engines like Google, to found sites that are vulnerable to a

certain kind of vulnerability. Among the different kinds of vulnerabilities to found, there are for instance: (i) "Vulnerable servers"; (ii) "Vulnerable files"; (iii) "Sensitive online shopping info"; (iv) "Network or vulnerability data"; (v) or "Pages containing login portals".

So, there are "Vulnerability repositories", "Exploit repositories", "Dork repositories", but there are more yet, there are operating systems specifically dedicated to hacking computer security systems, like "Kali Linux" available at "www.kali.org" and also frameworks that facilitate the reuse and development of exploits like "Metasploit" available at "github.com/rapid7/metasploit-framework" or "www.metasploit.com", but it comes already included inside Kali Linux. We can easily conclude that the operational resources for malicious uses of Internet are on the field and available to everyone.

Besides the operational resources refereed in last paragraphs, cyberspace also provides a native shield of protection due to its world wide geographical area, where at a distance of a mouse click we could order actions from one corner to any other corner of the world, giving to malicious cyberspace users the (i) "physical distance" and the (ii) "no need for visual contact" with their victims, shield of protection.

Science also plays a big role on malicious uses of cyberspace, because cryptography, namely "Public Key Cryptography" or "Asymmetric Cryptography" gives scientific support for Confidentiality, Authentication and also a secure way to negotiate a new key for cypher communications through the Diffie-Helman algorithm using intros case "Symmetric Cryptography" cyphers like the well known, secure and fast Advanced Encryption Standard (AES).

It is precisely this scientific support that gives rise to two of the most important technologies for malicious uses of cyberspace, namely: Anonym Communications; and Crypto Coins.

Nevertheless the possibility for establishment of anonym communications has a good principle that is the protection of private information about personal whishes and allows the protection of personal data. This same possibility, also allows the use of cyberspace with anonymization by those who have malicious intentions. This balance between personal data protection and the right to privacy from cyberspace users by one side, and fight malicious uses of cyberspace by other side, is for sure one of the biggest challenges for computer science and law communities in the coming years. Projects like "The Onion Router" (TOR) available at "www.torproject.org" which greatly contributes for dissemination of the DarkWeb use, allowing the browsing with anonymity and the publication of dangerous contents like drug selling, assassination by demand, guns market or pedophilia contents, among many others, strongly contributes for malicious uses of cyberspace. However, due to some lacks of the TOR protocol, its real anonymity has become questionable and new projects rise like the Riffle project available at "github.com/kwonalbert/riffle".

Crypto Coins, was first "thinking about" in late 1994 by the Cyberpunks group on a document named "The Cyphernomicon" as a dream of a Digital Cash and Net Commerce out of the dependency of Central Banks. In 2008 a paper entitled as "Bitcoin: A Peer-to-Peer Electronic Cash System" [1] published under the pseudonym "Satoshi Nakamoto" creates the first crypto coin. Bitcoins has genetically three main characteristics: (i) Cryptographic support with Asymmetric Cryptography; (ii) Validation of

transactions by a community of the so called “miners”, to which everyone could join using a specific protocol of transactions; (iii) High level of anonymization. Since then many other crypto coins was created based on Bitcoins original proposal. Nevertheless the use of Bitcoins should not be linked directly to malicious uses of cyberspace, indeed most of the cybercrime activities use Bitcoins as a way of payment. For instance the Europol report “Internet Organized Crime Threat Assessment 2015” [2], focused on the transaction payments for several cybercrimes and from the ten classes of cybercrimes listed there, Bitcoins was present at eight. Another perspective on this same study shows us that on “Victim Payments”, Bitcoins was in all the two kind of cybercrimes, on “Criminal to Criminal Payments”, Bitcoins was present in four of the six kind of cybercrimes, and Bitcoins was also present in the other two classes of cybercrimes related to “Payment for Legitimate Services” and “Money Movements”. It is however possible to pay with Bitcoins on several common days activities like on the “SubWay” food company or for ticket flights on “aBitSky” available at “www.abitsky.com” for instance. By other side, the number of crypto coins has been growing very fast. On April 21, 2016 there was 675 different kinds of crypto coins, on May 16, 2017 there was 722. By the time of this writing, September 2017 there are 867. Another interesting fact on crypto coins evolution is that, a special kinds of crypto coins, which main characteristic is the reinforce of the anonymization of the transactions, even more than Bitcoins, has been growing, the more commons are “Monero” available at “github.com/monero-project/monero” and “Dash” available at “github.com/dashpay/dash”, but recently in 2016 two others raised from the scientific community, namely “Zcoin” available at “github.com/zcoinofficial/zcoin” and “ZCash” available at “github.com/zcash/zcash”. There are also special applications to wash Bitcoin transactions like for instance the one available at “app.bitlaundry.com”. The Bitcoin transaction market is also an important point of analysis, because in the space of nearly one year and half, since April 2016, the Bitcoin value grows around ten times more. By April 21, 2016, one Bitcoin was around 381 Euros, by May 16, 2017, one Bitcoin was around 1607 Euros, and by the time of this writing, September 2017, one Bitcoin is stated at 3637 Euros. These values comes form the site “www.kraken.com”. Curiously this period, in the last one year and half, a special kind of cybercrime has gain particular attention, the “Ransomware” attacks that uses Bitcoins for payment from victims. Should it be a coincidence? We let this as a suggestion for a further reading. Finally about Bitcoins in particular, or crypto coins in general, there is a must to be refereed, which is its behind technology, named BlockChain, where Bitcoin transations are registered. In fact, this technology is a cryptographic supported way of chronological registration of property. With this technology, with this mechanism of registration of property its possible to assure the right of anything (not only crypto coins) and the validation of this right is done by all the community that wants to participate on the validation. The power of this technology could lead us to a world completely managed by machines, where they could register its property and make prove of it between anyone, machine or human – should this be considered a malicious use of cyberspace?

Finally we want to briefly focus on the use of cyberspace by terrorists [3]. As a mechanism of propaganda and training (recruitment, radicalization and incitation), online magazines such as “Dabiq” and “Rumiyah” form Islamic State or “Inspire” from al-Qaeda, are used to disseminate doctrine, glorification of heroic terrorist actions,

tutorials to build from scratch and with low cost materials of weapons. Computer games where the heroes are jihadist warriors, or platforms like the site "jihadology.net" where several activities and information are freely spread around the world. Terrorist groups have its owns cyphers like the "Asrar Al Dardashah", said as to was the first Islamic program for encryption instant messaging. As a funding support, by cause supporters or even by general society, or through cybercrime activities. As a planning platform, through the use of anonymization protocols at DarkWeb, to communicate between them or to obtain information from them targets. As a threat platform, with the possibility to disseminate fear through population. As an attack platform, with the possibility to affect not only cyberspace structures, as well as critical infra-structures that could affect populations and real world targets, from which we make a special appointment to the water distribution systems, due to its distribution to all populations houses, to its natural environment for biological virus propagation and also because it can not be stopped by one click due to its physical characteristics.

4 Conclusions

In this paper we briefly expose some of the malicious uses of cyberspace. We strongly believe that cyber security is strictly related with real hands on knowledge about the hackers procedures and technics. Cyber education, namely cyber security education is not only a must for technical stuff of companies and organizations, but also for every cyberspace user. The growing use of cyberspace for financial and e-government activities, relaying on cyberspace important issues of private and social modern societies, demands a fast and organized education about the risks of cyberspace. The two maxims of crime that says, "Where are the money, are the crime" and "Where are the people, are the crime", both apply to cyberspace, and the facts, some of which we point out in this paper, demonstrate the urgent need for a plan of cyber security education, from basic education to high school, to companies and organizations at all society. We believe that the better way to achieve this conscientiousness on population, is through demonstrations on hacker procedures, technics, resources, and also them way of thinking. This was our contribute on this paper, as a modest demand on a long path to a better and more secure cyberspace.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
2. Europol: Internet Organised Crime Threat Assessment 2015 (2016)
3. United Nations Office on Drugs and Crime: The Use of the Internet for Terrorist Purposes (2012)