IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 5, Issue 6, June 2017 ISSN 2321-5992

Cybersecurity Attacks: Common Vulnerabilities in the Critical Infrastructure

Sohail Razi Khan[1], Professor Luis Borges Gouvia[2]

[1]Sohail Razi Khan, University of Fernando Pessoa, Porto, Portugal

[2]Professor Luis Borges Gouvia, University of Fernando Pessoa, Porto, Portugal

ABSTRACT

The future of the digital economy relies upon the ability of cybersecurity technical solution with non-technical areas working in tandem with business units, executives, providers, and end-users to prevent any cyberattacks. In the recent many years there are multiple targeted cyberattacks carried against the critical infrastructures of a digital economy across the world. These cyberattacks have resulted in permanent or long term damage to the critical infrastructure and there is steady rise in the cyber and physical security related events that continue to raise the concerns. In this paper the attempt is made to identify the vulnerabilities that exist in the critical infrastructure that are exploited by the attacker to carry out a successful attack. The paper identifies software security vulnerabilities, poorly design networks, weak configuration vulnerabilities as a major vulnerabilities that are exploited to carry out successful attacks on the critical infrastructures. The paper identified non-technical vulnerabilities such as talent gap, budget constraints, lack of management priority and weak cyber security mechanism across various regions for a multi-national business that is spread across the globe as common vulnerabilities that are exploited for successful attacks on the critical infrastructure.

Keywords – Critical Infrastructure (CI), Cyber Attacks, Vulnerabilities, SCADA, Software, & Network design vulnerabilities.

1. INTRODUCTION

The inclusion of digital technology has improved business models and increases productivity and efficiency but at the sometime the risk to the critical infrastructure has increased and become more vulnerable to cyber threats McClimans (2016), Research Vice President, Cybersecurity & Digital Trust, HfS Research. Cyber-warfare unleashes massive scale attacks that can cause unrepairable consequences to their opponent's critical infrastructure leading to the disruption of the services and permanently damaging the reputation of the victim (Lewis, 2012). Critical infrastructure is crucial for any advanced country to maintain its competitive advantage. These infrastructure consist of information technology infrastructure running the finance and insurance services, transportation system, government services, energy, defense and health care systems which are considered as a backbone to any economy in the 21st century according to the Norton 2012 cybercrime report. The entire governmental or private operations can only function with stable and secure critical I.T infrastructure. In today's world, cyberattacks, network security, and breach to the confidential data highlights a complex problem and has a far reaching impact on the national security and public policy according to the Riptech Internet Security Threat Report, 2015. Any organization's computer system can be compromised in multiple ways such as a malicious or accidental action, worm, poorly written code or malfunction of the software components (Gellman, 2014). According to the report published by U.K government '2015 Information Security Breaches Survey', it concluded that 81% of large multinational companies have reported some form of security breach to their critical infrastructure, costing each organization on average between 600,000 and 1.5 million pounds sterling. The recent ransom attacks on NHS (National Health Services) in U.K and critical infrastructure across the world has shown a disturbing pattern showing how effective are these cyberattacks which are having massive disruption. Various examples of this disturbing pattern can be highlighted by the virus attacks on SCADA systems of the Iranian nuclear facilities, targeting telecommunication and power grid infrastructures of Estonia and Georgia (DeNileon & Guy, 2015). The growing trend to use information technology to support the critical infrastructures over the internet to reduce the overall cost and improve the efficiency has led to more exposure to these cyberattacks. Cybersecurity framework requires a rethinking of the entire strategy, and focus should move from protecting vulnerable assets to one that is directed towards strengthening critical infrastructures and assets. The framework required to integrate state-of-the-art

cybersecurity as an organizational policy that continuously evolves and adapts to the changing threat spectrum (McClimans, F., Fersht, P., Snowdon, J, 2016). This framework is not possible until we investigate and identify the common vulnerabilities in these critical infrastructures which allow these cyberattacks to attack place. This research paper is a comprehensive investigation study in-order to identify these vulnerabilities in the critical infrastructure that leads to the cyberattacks. Initially the paper highlights the cyberattacks on the critical infrastructure of various industries and provide examples of various types of successful attacks. The next section of the paper will group critical infrastructure vulnerabilities into different categories of vulnerabilities that exist in the infrastructure and are the cause of these successful cyberattacks. The paper discusses software vulnerabilities, network security issues, poor configuration management and non-technical issues that are major cause of successful attacks on the critical infrastructure.

2.Set the Context: A Brief Literature Review

2.1 Software Security Vulnerabilities

2.1.1 Improper Input Validation

The input validation is a technique to ensure an extra layer of security to prevent an attacker access to unintended functionality or privilege escalation DHS Recommend Practice Case Study: Cross-Site Scripting (2007). The input validation should only allow legitimate data to be entered into the system. The following section will detail attacks that can take place due to improper input validation.

2.1.2 Buffer Overflow

Due to lack of input validation the system can experience buffer overflow vulnerabilities that are due to the programming errors (Lewis, 2012). The main cause of this problem is that the programmer don't consider what could happen due to an input from the end-user such as user enters 2000 characters for last name. The problem occurs when the program is allowed to write more data into the buffer than the space allocated in the memory. Due to this the extra data is overwritten in the next memory ultimately resulting in crashing of the program. The attacker will exploit the successful memory overwritten by executing the code sent by the attacker. The exploit code allows the attacker to establish an interactive session and send commands with the privilege of the program with the buffer overflow. The problem that is fundamental to this issue is that the network protocols are implemented without the proper validation of input values and so these protocols are vulnerable to buffer overflow attacks. Due to poor coding practices that allows attackers inject unexpected data and thus modify the program execution. Due to buffer overflow various types of vulnerabilities can happen such stack-based or heap-based buffer overflow that allows remote code execution on the host.

2.1.3 Lack of Bound Checking

Due to lack of input validation which restrict the input to be at a certain range can result in program to crash and act in an unexecuted manner (Larissa, 2010). The invalidated input, very large numbers can be inserted into an array leading to the service to be crashed. Applications have suffered from coding practices that allow attackers to supply unexpected data and also modify the program execution.

2.1.4 Command Injection

In this type of attack the hacker inject commands and different codes for unauthorized execution. There are mainly two types of command injection Structured Query Language (SQL) injection and OS command injection. The malicious attacker will inject a semi colon that states the end of one command and start of another command (McClimans, Fersht, Snowdon, 2016). Data is inserted from a source that is untrusted and data is a part of a string that is executed as a command by the application. If the command is successfully executed the application will provide an attacker a privilege or capability that attacker was trying to seek in-order to compromise the system.

2.1.5 SQL Injection

Due to poor input validation the SQL command injection is most effective with database-driven websites. An attacker is able to inject a malicious scripts and website return value considering it was a legitimate request. The victim's web browser will execute the malicious scripts because it came from a server this will result in compromising the victim's computer by using one of many browsers exploits (Poulsen, 2003). This is caused by lack of data sanitization as most of

XSS stacks rely on user interaction and typically initiated from a link sent by the attacker. The end-user was misguided into clicking on the link since the link appeared to come from a respected entity and the user trust's that link. The malicious scripts is injected the attacker can perform variety of malicious activities. The attacker can send the malicious requests to the website on the behalf of the victim, can be dangerous if the victim has supervisory control privileges through that web application.

2.1.6 Improper Limitation of a Pathname to a Restricted Directory

Due to improper input validation the Directory traversal vulnerabilities occur when file paths are not validated. The directory traversal occurs when the software uses external inputs to construct a pathname that is intended to locate the file or directory that is a sub-directory to the parent directory. The attacker can read, overwrite, or create critical files such as programs, libraries, or important data. This attack will allow to execute unauthorized codes and run commands, modify the files and directories and crashed the important files leading to DoS (Denial of Service) attack.

2.1.7 Poor Code Quality

The attacker are successful to penetrate the critical infrastructures due to poor code quality that has not be carefully developed or maintained. These programs are vulnerable to attack as they don't follow secure development concepts and other good programming practices (Vijayan, 2008). The poor code quality is due to unsafe functions calls that the developer is responsible for validating the input. This leads to publicly announced buffer overflow and malformed input vulnerabilities which is a high risk to the validation. In the poor code quality the next issue that create major problem is the Null pointer dereference where the pointer is expected to be valid but this is NULL which leads to the program to crash unexpectedly. NULL pointer dereference is usually result in the failure of the process unless exception handling is available and implemented.

2.1.8 Permission, Privileges, and Access Controls

According to Cybersecurity Strategy for European Union presented by European Commission in 2013, the attack take place in the critical infrastructure due to lack of permission, privileges and access control on the systems. The attack is initiated leading to gain access to unauthorized access. Due to improper access control and checks across all potential execution paths the unauthorized users are able to access data or perform actions that are not legitimate. The attack will exploit the vulnerability where the access is not restricted to the objects, common shares are available on multiple systems, lack of role-based authentication, and remote users can imitate any process without authorization where they can upload the files to any locations on the targeted computer without any restrictions. The attacker will exploit the system using the undisclosed "back door" to gain access and remain anonymous over the network. The system never follows the principals of least privileges where the user can have multiple accounts for functions that require different level of privileges and default configuration is not changed. Due to unnecessary privileges the attacker gain access to the network and then tries privilege escalation to exploit the vulnerable service running. The full access will allow the attacker to inflict huge damages that will affect the entire operations.

2.1.9 Improper Authentication

The next attack that takes place on the critical infrastructure is due to improper authentication mechanism. Due to poorly designed software the mechanism doesn't verify the claim of the given identity as mentioned by the report "Information Security Breaches, 2014" presented by GCHQ, U.K. The report identifies that the protocols design ensures that how authentication, integrity checks, and confidentiality will be implemented. The service deploys weak authentication methods can be exploited to gain unauthorized access and escalate the privileges. The software doesn't perform authentication allowing it to be bypassed through various methods. The attacker exploit situation where the application allows the authentication of users to be taken at a local level where information needed to authenticate is stored on the client side. The attacker will extract the information or modify the client credentials so that it doesn't require authentication. For a successful attack the attackers can bypass the client-side checks by modifying values after the check have been performed or completely removing the client-side checks from the system. Then modified values are sent to the server for perform illegal transaction. Due to improper authentication MitM (Man-in-The-Middle) attack is possible as we have not adequately verify the identity of end-users over the communication channel nor we were able to ensure the integrity of the channel. This weakness will allow cyberattacks on the critical infrastructure.

2.1.10 Insufficient Verification of Data Authenticity

The attack that can affect the critical infrastructure is due to insufficient verification of data authenticity. The Cross-Site Request Forgery (CSRF) can affect the operation where the web server is bound to receive requests from a client without any mechanism for verifying that it was intentionally sent. The attack is initiated by the attacker to trick a client into making an unintentional request to the web server that will be treated as an authentic request. The attack will allow the hacker to change the settings and hijack the credentials by using the cross-site request forgery (CSRF) which will give the ability to perform any task just as an authorized user will be able to do so (Gellman, 2014). There are many transmission protocols that doesn't include the mechanism to verify the integrity of the data during transmission. These protocols don't have checksums value so there is no way of finding if the data is correct or has been corrupted during the transmission. Due to lack of checksum functionality the protocol removes the first application-level check of data that can be used. By excluding the checksum value the data can't be validated leading to malicious alteration during the transmission of data. The next type of attack can take place if the source code or an executable code is executed without sufficiently verifying the origin and integrity of the code. The attacker can attack the critical infrastructure by executing a malicious code so that they can compromise the host server, spoofing an authorized server or can modify the data while it was in transit.

2.1.11 Cryptographic Issues

The data sent over the network requires a strong encryption so that unauthorized access can be restricted. If the data is sent over the network without strong encryption then attacker will be able to capture usernames and password because the data is sent in clear. Most of the attacks that take place on the critical infrastructure are due to weak or unencrypted plain-text network on these communication protocols. It has been reported widely that many applications and services are using protocols that don't use string encryption and includes human-readable characters and strings which hackers can easily access. Various network sniffing tools are used to monitor the traffic, packets are intercepted and manipulated. These attacks are successful because weak hashing algorithm, poorly designed pseudorandom number generation and vulnerable unpatched secure sockets layers (SSL) libraries are deployed with wireless devices.

2.1.12 Security Configuration and Maintenance

Attacks on the critical infrastructure can take place due to vulnerabilities in the software security configuration, poor maintenance of different platforms such as hardware, operating systems, and various applications. The computer system are vulnerable to these attacks from the time of vulnerability is discovered and until the patch is generated and applied to close that gap. Due to poorly designed software' nowadays the publicly announced vulnerabilities has been steadily increased and patch management is become a crucial part to maintain the systems. The attacks are successful because unpatched or old version of applications still being used without updating the system. These old applications possess vulnerabilities that provides an opportunity to the attacker to exploit these codes and target the critical infrastructures. The common problem that leads to successful attacks on the critical infrastructure is due to lack of secure authentication applications were used where configuration setting were not secure enough to protect against these attacks. Security functions were not integrated during the software development cycle and which is loophole exploited by hackers to penetrate into the systems.

2.2 Network Security Vulnerabilities

The network architecture needs to be securely designed to allow remote access and monitoring for all business processes while stopping any unauthorized traffic from entering the networks. Security zones with access control rules that can provide an extra layer of security to limit the traffic allowed in and out of the zone and reduce the intention or unintentional attacks. In the following section following attacks that can take place on the critical infrastructure due to the weakness in the Network Security are detailed.

2.2.1 Poor Network Design

Poorly design network that don't deploy defense in-depth strategy is major cause of attacks on the critical infrastructure. The networks don't deploy multiple layers of security and use flat networks without any perimeters or zones, no use of port security and poor remote access policies are a major weakness due to which successful attacks take place (DeNileon & Guy, 2015). To make the problem even worse is that these networks are directly connected to the corporate environment without firewalls and DMZ zones providing direct access to the Internet. Poor design networks allow the hackers to conduct successful attacks on the critical infrastructure.

2.2.2 Security Perimeter Defined Boundaries

The networks should define clearly the security perimeter to defend against any type of attack. The network security perimeter should be logically separated from the corporate network on physical separated network devices and additional network security controls should be on-place to prevent intrusion. As the security perimeters are not clearly defines this leads to unauthorized access to the system and data as well.

2.2.3 Lack of Network Segmentation

Due to minimal or no security zones it allows exploitation to gain full control of the system which can lead to massive consequences. The lack of internal segmentation where the Inter-Control Center Communication protocol (ICCP) servers are not in the DMZ servers (Gellman, 2014). Also dedicated serial links for sensitive transfer of data are using applications that are not within the DMZ which is major weakness and leads to successful attacks.

2.2.4 Firewall Issues

The lack of properly configured firewalls will allow unauthorized data to pass between the networks without any proper checks. Successful attacks on the critical infrastructures take place due to poorly configured or nonexistent firewalls which can allow malwares and virus to spread between networks. Poorly configured firewalls allows the compromise of confidential data which can be monitored or accessed by unauthorized individuals (Lewis, 2012). As the firewalls are poorly configured there are examples of multiple instances where connection to and from a remote facilities doesn't pass through the firewall and is a major reason to the successful attacks.

2.3 Configuration Vulnerabilities

The attack on the critical infrastructure takes place as the network devices are not configured properly to prevent any unauthorized access. The network devices access control list are not configured properly and doesn't restrict the access by unauthorized users. The other major weakness that allows attacker to carry out a successful attack is the remote access to these network devices in the clear-text without using encryption or proper authentication protocol. These extra layer of restriction is required to prevent hackers to achieve root access to these devices and eventually change the network device configuration.

2.3.1 Permission, Privilege, and Access Controls

The major reason for the successful attacks on the critical infrastructure is due to lack of policies on permission and access controls. The lack of separation of duties, no existence of lockout of system enforcement for failed login attempt, and no mechanism to terminate remote access session after a period of time leads to the successful attacks on the critical infrastructure.

2.3.2 Improper Authentication

Weak or no proper authentication with lack of policies or procedures have allowed the attacks to take place on the critical infrastructure. Organization lack the formal documentation that states that authentication policies and controls and doesn't uniquely identify how to authenticate users and specify devices before establishing connection. Due to weak authentication policies the system fails to uniquely identify and authenticate users and there is no mechanism of providing authentication on role-based, group-based, or device-based. The organization needs to manage users uniquely, verify their identity, and receive authorization to provide a user with proper authentication to access the system.

2.3.3 Credential Control Management

According to MITRE, (2015) "Common Attack Pattern Enumeration and Classification (CAPEC), the credential related to the authorized users should be protected from the attackers. The attackers will be able to see the credentials passed over the networks in the clear text. If the passwords are not properly hashed and encrypted they can be accessed from the hackers leading to gaining full access privilege to inflict a major damage over the network. Services such as FTP, telnet and rlogin transmit the user credential in the clear text that is vulnerable to the attack. The database service configuration allowed administrator passwords to be displayed on the web pages and password hash files are not properly secured leading to the attacks on the critical infrastructure.

2.3.4 Security Configuration and Maintenance

One of the major vulnerabilities in a system in an unpatched software which is not being maintenance or tested properly. The successful attacks takes place on the critical infrastructure as the operating system updated patches are not applied, system computers are vulnerable to the operating system service vulnerabilities, and using outdated version. These updates have to be applied on a timely basis to avoid any attacks on the systems.

2.3.5 Weak backup and Restore Functions

Backup and restoring the backup is a major requirement for continuing the operation in an event for an incident. There is a need of a comprehensive policy to make backup, have a policy to store these backup at safe and offsite location and to test these backup on a regular basis is crucial for continuation of the operation. In many cases backup are made but there is no consistent policy on storing these backup and testing the backups. The integrity and availability are the main concern related to the backup information, protecting backup information from unauthorized disclosure is also an important consideration which if not considered can lead to attacks on the critical infrastructure.

2.3.6 Weak Port Security

The unauthorized network access is possible due to weak port security which the attackers always exploit. Due to weak port security there is easy access to the hardware interfaces. The malicious users who has physical access to an unsecured port on a network switch could easily plug into the network behind the firewall to defeat its incoming filtering protection. The weak port security can't prevent the change of MAC addresses and new unauthorized devices to be introduced over the networks without authorization.

2.3.7 Poor Monitoring of IDS

The other reason for successful attacks on the critical infrastructure is that good cybersecurity practices to monitor the IDS (Intrusion Detection System) and make corrective decision to prevent any threats are not be followed. The network-based IDS/IPS or host-based IDS/IPS are not deployed to effectively monitor the traffic.

2.4 Cyber Gaps: Non-Technical Challenges

In this section of the paper the non-technical challenges that an organization is facing due to cyber security threat will be detailed. Various researchers have identified significant gaps that are hindering the ability to protect against the target cyberattacks. The failure to proactively address these gaps has weaken the enterprise security and increased the risk to the enterprise networks.

2.4.1 Talent Gap

As the cyber threats is becoming serious challenge for businesses across the world there is a growing gap between the technical and operational skills set that are required and the pool of talent that is available to offer their services. Due to this talent gap the organization are not able to defend against the growing cyberattacks. According to the survey conducted with 218 enterprise "The State of Cybersecurity and Digital Trust 2016", Accenture and HIS Research, more than 72% of staff need more training for identity/privacy issues whereas 76% of staff require updating of skills in threat and vulnerability assessments and 74% needs more training in device security and application security issues. The survey highlighted that 77% of staff need more training to understand the issues related to GDPR (General Data Protection Regulation) and 76% of staff require help in improving data integrity issues. The talent gap is real and continues to grow which is major concern for enterprise cybersecurity team and can lead to the cyberattacks on the critical infrastructure.

2.4.2 Budget Constraints

There is a budget constraint to defend against various cyberattacks. The budget constraints has become a real challenge due to management focus, organization priorities, financial realities and lack of actual resources required to secure the enterprise which are depleting due to other constraints global business constraints. According to the survey conducted with 218 enterprise "The State of Cybersecurity and Digital Trust 2016", Accenture and HIS Research, only 42% of organization believe that they have enough budget for technology but need additional security talent and training whereas 26% of organization believe that they have enough budget for both technology and enough security staff. 16% of organization stated they have enough budget for well-trained staff whereas 12% of surveyed organization stated that they have not enough budget allocation for rising threats or being asked to cut the back on the expenses that can lead to cyberattacks.

2.4.3 Priority of the Management

At the moment there is a huge perception gap that exist between the executive management and security operation management. This gap has to be addressed so that the cyber threat should be considered by the management as the top priority for the continuity of the business operations. The challenge lies in the gaps that are revealed between security operations and executive management. According to the survey conducted by "The State of Cybersecurity and Digital Trust 2016", Accenture and HIS Research, 35% of respondent believe management are not concerned with security issues and whereas 36% respondents believe that the management consider security an unnecessary cost.

2.4.4 Parity Gap

As it a norm for businesses to have multinational operations across various continents across the globe. The gap in cyber readiness among various regions where these multi-national businesses are working is considered as a major risk and can affect the entire operation.

3.Conclusion

Critical infrastructure is crucial for any advanced country to maintain its competitive advantage. These infrastructure are considered as the backbone for any advanced economy. The risk to computer systems and information comes from a wide range of spectrum of threats such as software vulnerabilities, poorly design network, device misconfiguration issues, and non-technical challenges such as budget constraints and lack of available technical skills to match the requirements of various businesses. The impact of these attacks on different businesses will depend on the opportunities you provide to the attackers' in-terms of vulnerabilities that are within the system and the capability of the attackers to exploit these vulnerabilities. Various vulnerabilities exist in the systems in the form of software vulnerabilities such as improper input validation, buffer overflow, poor code quality, improper authentication, cryptographic issues, and insufficient verification of data authenticity that can cause successful attack on the critical infrastructure. The next vulnerability that can lead to successful attacks on the critical infrastructure is due to poorly design networks. The network architecture needs to be securely designed to allow remote access and monitoring for all business processes while stopping any unauthorized traffic from entering the networks. Security zones with access control rules that can provide an extra layer of security to limit the traffic allowed in and out of the zone and reduce the intention or unintentional attacks. The attack on the critical infrastructure takes place due to poor configuration of the network devices as they are not configured properly to prevent any unauthorized access. The network devices access control list are not configured properly and doesn't restrict the access by unauthorized users leading to attacks in the critical infrastructure. There are many other non-technical vulnerabilities that can lead to the successful attacks such as Talent gap where there is a growing gap between the technical and operational skills set that are required and the pool of talent that is available to offer their services. The budget constraints has become a real challenge due to management focus, organization priorities, financial realities and lack of actual resources required to secure the enterprise which are depleting due to global business constraints. At the moment there is a huge perception gap that exist between the executive management and security operation management. The gap in cyber readiness among various regions where these multi-national businesses are working is considered as a major vulnerability that allows attacks on the critical infrastructure. Until these vulnerabilities are not resolved the critical infrastructure will be prone to successful attacks.

References

[1]. DHS CSSP, (2009), Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments, July 2009, http://www.uscert. gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08-14750_Final_7-1-09.pdf.

[2]. McClimans, F., Fersht, P., Snowdon, J., (2016), "The State of Cybersecurity and Digital Trust, 2016", HfS Research &Accenture, Ltd

[3]. Information Security Breaches, GCHQ (2014), www.gov.uk/government/publications/information-security-breaches-survey-2014.

[4]. ANSI/ISA–99.(2007), Security for Industrial Automation and Control Systems Part 1:

[5]. Terminology, Concepts, and Models, October 2007, pages 69–73.

[6]. DHS, DHS Recommended Practice Case Study: Cross-Site Scripting, February 2007, http://www.uscert.gov/control_systems/practices/documents/xss_10-24-07_Final.pdf, Web page last accessed May 2017.

[7]. Lewis, J, (2012), "Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats: Center for Strategic and International Studies, Washington, DC.

[8]. Gellman, B. (2014) "Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2014
[9]. Larissa, P (2010), "When Cyber Hacktivism Meets Cyberterrorism," SANS Institute, "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding"
[10]. Segan, S, (2000) "Safety At Risk, " ABC News.com, September 27, 2000,
[11]. DeNileon & Guy, (2015), "The Who, What Why and How of Counter-terrorism Issues," American Water Works Association Journal, May 2015, Volume 93, No. 5, pp. 78–85
[12]. MITRE, CWE (Common Weaknesses Enumeration), http://cwe.mitre.org/, Web page last accessed March 2017.
[13]. Poulsen, K. (2003), "Slammer worm crashed Ohio nuke plant network, August 2003",
[14]. http://www.securityfocus.com/news/6767, Web page last accessed April 2017.
[15]. DHS CSSP, (2009), Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, October 2009, http://www.uscert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf, Web page last accessed April 2017.
[16]. Vijayan, J. (2008), Gates pushed change in security culture at Microsoft, June 2008,
[17]. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9102998, Web page last accessed May 2017.
[18]. MITRE, (2015), Common Attack Pattern Enumeration and Classification (CAPEC), http://capec.mitre.org/, Web page last accessed February 2017. Weapons of mass annoyance: a phrase originated by Stewart Baker.
[19]. Barton Gellman, (2012) "Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool," The Washington Post, June 27, 2012
[20]. Network of Excellence (NESoS), (2012), Deliverable: Selection and Documentation of the Two Major Application Case Studies. Springer Lecture Notes in Computer Science.
[21]. Norton 2012 cybercrime report - italy. http://now-static.norton. com/now/en/pu/images/Promotions/2012/cybercrimeReport/NCRCountry_Fact_Sheet-Italy.pdf, 2012.
[22]. Cybersecurity strategy of the european union: An open, safe and secure cyberspace. European Commission, Brussels, JOIN(2013) 1 final, 2013. Noi Italia. 100 statistiche per capire il paese in cui viviamo. ISTAT,
[23]. Riptech Internet Security Threat Report, (July 2015), http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf Testimony of Michehl R. Gent Before the Senate Government Affairs Committee, May 8, 2002, ftp://www.nerc.com/pub/sys/all_updl/docs/testimony/mrg-testimony-SenateGovernmentalAffairs-5-08-02-(final).pdf

Author

Sohail Razi Khan received MSc (Distributed Networks and Security System) from University of Hertfordshire, M.A in (Education and Leadership) from University of Wolverhampton and MBA in (Business Administration) from University of Central Lancashire, from England. Mr. Khan is involved in teaching computer science in higher education institutions from last 12 years and currently pursuing his PHD (Doctor of Philosophy) in the field of Cloud computing and Data Security issues. Mr. Khan has worked as a IT strategy consultant providing advice and solutions for business enterprise as well.

Professor Luis Borges Gouvia has extensive experience in academics, monitoring various researches, publication of various books and contributed extensively in latest research in the field of cloud computing, cyber security, E-Commerce and Web 2.0 and Higher Education. Professor Gouvia, has PHD (Doctor of Philosophy), from University of Lancaster, England. He is a full professor in University of Fernando Pessoa, Porto, Portugal and successfully supervised various PHD students.