NETWORK SECURITY ATTACKS, IMPACT AND COUNTERMEASURES

Deepika Aggarwal[*]

***Abstract*—** Due to widespread usage of internet over the network and the advancement of internet technologies where the growing threat of network attacks has increased, network security has become critical requirement for everyone. Various security measures are being taken to fight against these attacks. This paper outlines various network security attacks, their impacts and countermeasures.

Key Terms: Social engineering, Dos and DDos attack, MITM attack, SQL Injection attack, XSS attack.

[*] Department of Computer Science and IT, DAV College Chandigarh, Panjab University, India

I. Introduction

Network security attack is usually defined as an intrusion on the network infrastructure that will first analyse the environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to system resources. In such cases where the purpose of attack is only to learn and get some information from the system but the system resources are not altered or disabled in any way, such attacks are known as Passive attacks. Active attack occurs where the perpetrator accesses and either alters, disables or destroys system resources or data. Attack can be performed either from outside of the organization by unauthorized entity (Outside Attack) or from within the company by an "insider" that already has certain access to the network (Inside Attack) [1].

A network consists of routers from which information can easily be stolen by the use of malwares such as Zeus and SpyEye. The synchronous network consists of switches and since they do not buffer any data and hence are not required to be protected. Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. Some new trends are emerging: some are based on old ideas such as biometric scanning while others are completely new and revolutionary. Email is a widely used service today and it also contains many serious flaws, there is no system of authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can easily be intercepted and changed. SPAM are serious security threats as they only require very less manpower but can affect millions to billions of Email users around the world, they can either be malicious links or even false advertisements. A network contains much vulnerability but most of them can be fixed by following very simple procedures, such as updating software and correctly configuring network and firewall rules, using a good anti-virus software etc [2]. This paper discusses various types of network security attacks like social engineering, DOS and DDOS, MITM, SQL injection and XSS, also outlines their impacts and countermeasures.

II. Types of Network Security Attacks and Impact

We can group network attacks by the skills possessed by the attacker. Based on this criterion we can divide attacks in two categories:

Unstructured Attacks – These attacks are made by unskilled hackers. Individuals behind these attacks use hacking tools available on the Internet and are often not aware of the environment they are attacking. These threats should not be neglected because they can expose precious information to malicious users.

Structured Attacks – These attacks are made by individuals who possess advanced computing skills. Such hackers are experts in exploiting system vulnerabilities. By gaining enough information about a company's network, these individuals can create custom hacking tools to breach network security. Most structured attacks are done by individuals with good programming skills and a good understanding of operating systems, networking and so on. [3]

Depending on the procedures used during the attack or the type of vulnerabilities exploited, the network attacks can be classified in following ways:

A. SOCIAL ENGINEERING

Social engineering is an art of manipulating people so that they give up their confidential information. The types of information these criminals seek can vary, but when individuals are targeted the criminals usually try to trick the people to get their passwords or bank information, or access to their computer to secretly install malicious software. Criminals use social engineering tactics because it is usually easier to exploit person's natural inclination to trust than it is to discover ways to hack ones software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak) [4]. All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases. These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques, which are listed ahead [5].

Common social engineering attacks –

1) *Email from a friend:* If a criminal manages to hack or socially engineer one person's email password then he gets access to that person's contact list–and because most people use one password everywhere, then criminal probably have access to that person's social networking contacts as well, thereby criminal may send emails to all the person's contacts or leave messages on all his friend's social pages, and possibly on the pages of the person's friend's friends. These messages may use one's trust and curiosity, because such messages may contain a link, a download, may urgently ask for help or may ask for donation to their charitable fundraiser, or some other cause which if a person responds to, then system of that person will get infected with malware. [4]

2) *Phishing attempts:* It is an attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing (creation of email messages with a forged sender address [16]) or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one [6]. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless a link provided was clicked to update a credit card (information that the genuine eBay already had). Because it is relatively simple to make a Web site resemble a legitimate organization's site by mimicking the HTML code, the scam counted on people being tricked into thinking they were being contacted by eBay and subsequently, were going to eBay's site to update their account information. By spamming large groups of people, the Phisher counted on the e-mail being read by a percentage of people who already had listed credit card numbers with eBay legitimately, who might respond. [4]

3) *Baiting Scenarios:* Baiting in many ways is similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that hackers use to entice victims. These social engineering schemes know that if something is dangled which people want, many people will take the bait. Baiters may offer users free music or movie downloads, if they surrender their login credentials to a certain site. Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media. One such attack was documented by Steve Stasiukonis, VP and founder of Secure Network Technologies, Inc., back in 2006. To assess the security of a financial client, Steve and his team infected dozens of USBs with a Trojan virus and dispersed them around the organization’s parking lot. Many of the client’s employees picked up the USBs and plugged them into their computers, which activated a keylogger and gave Steve access to a number of employees’ login credentials.[4][7]

4) *Quid Pro Quo:* Quid pro quo means something for something. These attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting frequently takes the form of a good. One of the most common types of quid pro quo attacks involve fraudsters who impersonate IT service people and who spam call as many direct numbers that belong to a company as they can find. These attackers offer IT assistance

to each and every one of their victims. The fraudsters will promise a quick fix in exchange for the employee disabling their AV program and for installing malware on their computers that assumes the guise of software updates. As real world examples have shown, in a 2003 information security survey, 90% of office workers gave researchers what they claimed was their password in answer to a survey question in exchange for a cheap pen. Similar surveys in later years obtained similar results using chocolates and other cheap lures, although they made no attempt to validate the passwords. [7][5]

5) *Tailgating:* This social engineering attack type is also known as piggybacking. These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area. In a common type of tailgating attack, a person impersonates a delivery driver and waits outside a building. When an employee gains security's approval and opens the door, the attacker asks that the employee hold the door, thereby gaining access off of someone who is authorized to enter the company. Tailgating does not work in all corporate settings, such as in larger companies where all persons entering a building are required to swipe a card. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to successfully get past the front desk. In fact, Colin Greenless, a security consultant at Siemens Enterprise Communications, used these same tactics to gain access to several different floors, as well as the data room at an FTSE-listed financial firm. He was even able to base himself in a third floor meeting room, out of which he worked for several days [7].

6) *Pretexting:* It is also known in the UK as blagging or bohoing. It is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances [5][8]. This technique can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives [5][9]. The information can then be used to establish even greater legitimacy under tougher questioning with a manager, *e.g.*, to make account changes, get specific balances, etc. Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. Unlike phishing emails, which use fear and

urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target [7].

7) *Diversion Theft:* It is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the persons responsible for a legitimate delivery that the consignment is requested elsewhere, near to or away from, the consignee's address, in the pretense that it is "going straight out" or "urgently required somewhere else" — hence it is called "round the corner" [5].

B. DOS AND DDOS ATTACK

Denial of Service Attack (DoS Attack) [1] is designed to cause an interruption or suspension of services of a specific host/server by flooding it with large quantities of useless traffic or external communication requests. When the DoS attack succeeds the server is not able to answer even to legitimate requests any more - this can be observed in numbers of ways: slow response of the server, slow network performance, unavailability of software or web page, inability to access data, website or other resources. Distributed Denial of Service Attack (DDoS) occurs where multiple compromised or infected systems, called Botnet, flood a particular host with traffic simultaneously.

Most common types of Dos attack are as follows:

1) *ICMP flood attack (Ping Flood)*: The attack that sends ICMP (Internet Control Message Protocol) ping requests to the victim host without waiting for the answer in order to overload it with ICMP traffic to the point where the host cannot answer to them any more either because of the network bandwidth congestion with ICMP packets (both requests and replies) or high CPU utilisation caused by processing the ICMP requests. Easiest way to protect against various types of ICMP flood attacks is either to disable propagation of ICMP traffic sent to broadcast address on the router or disable ICMP traffic on the firewall level.

2) *Ping of Death (PoD)***:** This attack involves sending a malformed or otherwise corrupted malicious ping to the host machine - for example PING having big size can cause buffer overflow on the system leading to a system crash.

3) *Smurf Attack***:** It works in the same way as Ping Flood attack with one major difference that the source IP address of the attacker host is spoofed with IP address of other legitimate non malicious computer. Such attack will cause disruption both on the attacked host (receiving

large number of ICMP requests) as well as on the spoofed victim host (receiving large number of ICMP replies).

4) *SYN flood attack:* It exploits the way the TCP 3-way handshake works during the TCP connection is being established. In normal process the host computer sends a TCP SYN packet to the remote host requesting a connection. The remote host answers with a TCP SYN-ACK packet confirming the connection can be made. As soon, this is received by the first local host it replies again with TCP ACK packet to the remote host. At this point the TCP socket connection is established. During the SYN Flood attack the attacker host or more commonly several attacker hosts send SYN Packets to the victim host requesting a connection, the victim host responds with SYN-ACK packets but the attacker host never respond back with ACK packets - as a result the victim host is reserving the space for all those connections still awaiting the remote attacker hosts to respond - which never happens. This keeps the server with dead open connections and in the end effect prevent legitimate host to connect to the server any more.

5) *Buffer Overflow Attack:* In this type of attack the victim host is being provided with traffic/data that is out of range of the processing specs of the victim host, protocols or applications - overflowing the buffer and overwriting the adjacent memory. One example can be the mentioned Ping of Death attack - where malformed ICMP packet with size exceeding the normal value can cause the buffer overflow.

C. MAN-IN-THE-MIDDLE ATTACK

It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe that they are directly communicating with each other [10]. The man-in-the middle (abbreviated as MITM, MitM, MIM, MiM or MITMA) attack intercepts a communication between two systems. One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in Fig. 1. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication. The MITM attack is very effective because of the nature of the http protocol and data transfer which are all ASCII based. In this way, it's possible to view and interview within the http protocol and also in the data transferred.

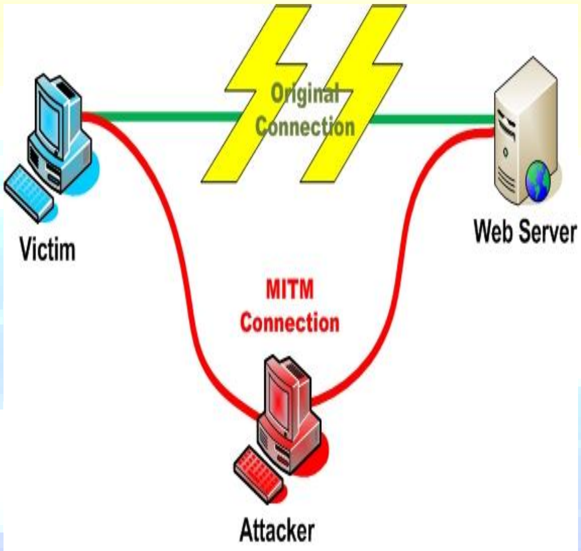

Fig. 1 Splitting of TCP connection into two new connections

D. SQL INJECTION ATTACK

SQL injection attack as shown in Fig. 2 could allow hackers to compromise your network, access and destroy your data, and take control of your machines. In this attack, attacker uses existing vulnerabilities in the applications to inject a code/string for execution that exceeds the allowed and expected input to the SQL database [1]. For example, when an application takes user data as an input, there is an opportunity for a malicious user to enter carefully crafted data that causes the input to be interpreted as part of a SQL query instead of data [11].

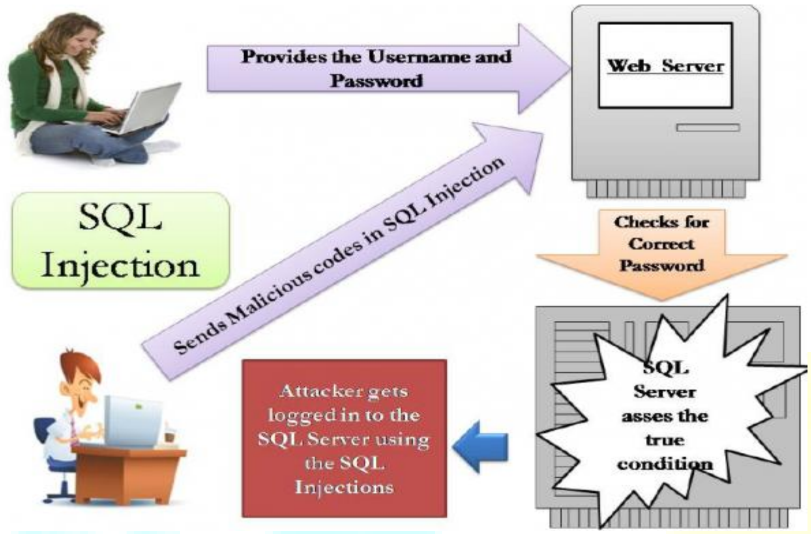
Provides the Username and Password
Web Server
SQL Injection
Sends Malicious codes in SQL Injection
Checks for Correct Password
SQL Server asses the true condition
Attacker gets logged in to the SQL Server using the SQL Injections

Fig. 2 SQL Injection attack

E. XSS ATTACK

Cross-Site Scripting (XSS) attacks are a type of injection, in which the attacker exploits the XSS vulnerabilities found in Web Server applications in order to inject malicious client-side script onto the webpage of trusted website that can either point the user to a malicious website of the attacker or allow attacker to steal the user's session cookie.

Fig. 3 shows how an attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks, the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page [1][13].

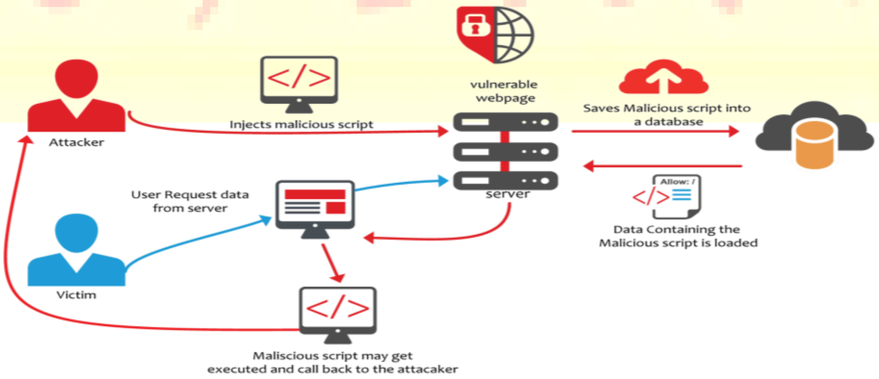
vulnerable webpage
Attacker
Injects malicious script
Saves Malicious script into a database
server
User Request data from server
Allow: /
Data Containing the Malicious script is loaded
Victim
Maliscious script may get executed and call back to the attacaker

Fig. 3 XSS Attack

III. Countermeasures for Combating Network Security Attacks

In network security a countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. Some common countermeasures for combating network security attacks are listed in the following sections:

A. COUNTERMEASURES FOR SOCIAL ENGINEERING

A proper countermeasure training program should include the following measures:

1) *Conduct a data classification assessment:* Identify which employees have access to what types and levels of sensitive company information and know who the primary targets of a social engineering scheme are likely to be.
2) *Never release confidential or sensitive information:* to unknown person or who doesn't have a valid reason for having it- even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email.
3) *Establish procedures:* to verify incoming checks and ensure clearance prior to transferring any money by wire and to verify any changes to customer or vendor details, independent of the requester of the change.
4) *Reduce the reliance:* on email for financial transactions. If email must be used, establish call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.
5) *Avoid using or exploring "rogue devices":* such as unauthenticated thumb/ flash drives or software on a computer or network.
6) *Be suspicious of unsolicited emails:* only open those from trusted sources. Never forward, respond to or access attachments or links in such emails, delete or quarantine them.
7) *Avoid responding to any offers made over the phone or via email:* If it sounds too good to be true, then it probably is. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter.
8) *Be cautious in situations where a party refuses to provide basic information:* Attempt to rush a conversation (act now, think later), uses intimidating language or requests confidential information.

9) *Always shred and/ or destroy:* physical documents and other tangible material such as computer hardware and software prior to disposal in any on-site receptacles, such as dumpsters.

10) *Proactively combat information security complacency:* in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalogue incidents of social engineering and implementing an incident-response strategy.

11) *Train customer service staff:* to recognize psychological methods that social engineers use such as power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it is important enough to verify.

12) *Consider conducting a recurring, third-party penetration test:* to assess organization's vulnerability, including unannounced random calls or emails to employees soliciting information that should not be shared.

13) *Guard against unauthorized physical access:* by maintaining strict policies on displaying security badges and other credentials and making sure all guests are escorted. Politely refuse entry to anyone "tailgating". Keep sensitive areas, such as server rooms, phone closets, mail rooms and executive offices, secured at all times.

14) *Monitor use of social media outlets, open sources and online commercial information:* to prevent sensitive information from being posted on the internet.

The best defense for combating social engineering fraud is awareness through corporate culture, education and training. It is not enough for a workforce to simply follow a policy guideline, employees must be educated on how to recognize and respond to an attacker's methods and thus become a "human firewall" [14].

B. COUNTERMEASURES FOR DOS AND DDOS ATTACK

Many technologies have been developed to prevent Dos and DDoS attacks such as Intrusion Detection Systems (IDSs), firewalls, and enhanced routers. All the above specified things are used between internet and server. They protect the network by monitoring all incoming and outgoing connections. These technologies contain traffic analysis, access control and redundancy features. IDSs maintain a log for incoming and outgoing connections and to detect potential Dos attack, maintained log is then compared to the baseline traffic, if there is unusually high traffic on the server then specified techniques can also alert the system of a possible ongoing DOS attack such as TCP SYN flooding. Firewalls can also be used as defence against DOS attacks with the required configuration. Firewalls can be used to allow or deny certain packets, ports and IP addresses etc. Firewalls can also perform real time evaluation of the traffic and take the necessary steps to prevent the attack. Security measures can also be employed in routers which can create another defence line away from the target, so even if a DOS attack takes place it won't affect the internal network. Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible. If the service providers are able to distribute the heavy traffic of a DOS attack over a wide network quickly it can also prevent DOS attacks, however this method require computer and network resources and they can be very costly to provide on daily basis as a result only very big companies opt for this method [2].

C. COUNTERMEASURES FOR MAN-IN-THE-MIDDLE ATTACK

1) *Use cryptography*: If data is encrypted before its transmission, the attacker can still intercept it but cannot read it or alter it. If the attacker cannot read it, he or she cannot know which parts to alter. If the attacker blindly modifies the encrypted message, then the original recipient is unable to successfully decrypt it and, as a result, knows that it has been tampered with.
2) *Use Hashed Message Authentication Codes (HMACs)*: If an attacker alters the message, the recalculation of the HMAC at the recipient fails and the data can be rejected as invalid [15].

D. COUNTERMEASURES FOR SQL INJECTION ATTACK

1) *Perform thorough input validation:* Application should validate its input prior to sending a request to the database.
2) *Use parameterized stored procedures:* for database access to ensure that input strings are not treated as executable statements. If stored procedures cannot be used, then SQL parameters can be used while building SQL commands.
3) *Use least privileged accounts:* to connect to the database [15].

E. COUNTERMEASURES FOR XSS ATTACK

1) *Perform thorough input validation:* Your applications must ensure that input from query strings, form fields, and cookies are valid for the application. Consider all users input as possibly malicious, and filter or sanitize for the context of the downstream code. Validate all input for known valid values and then reject all other input. Use regular expressions to validate input data received via HTML form fields, cookies, and query strings.

2) *Use HTMLEncode and URLEncode functions:* to encode any output that include user input. This converts executable script into harmless HTML [15].

IV. Conclusion

As the use of the Internet is becoming increasingly popular, more and more people are becoming aware of some of the vulnerabilities at hand, therefore, the number of attacks is rising day by day. Cybercriminals are becoming more sophisticated and collaborative with every coming year. To combat the threat in current and future years, information security professionals must think about security policies and where and how to provide protection. The network security field will have to evolve more rapidly to deal with the threats further in the future.

References:

[1] "Symantec: Various types of network attacks", http://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks.

[2] Kartikey Agarwal, Dr. Sanjay Kumar Dubey, "Network Security : Attacks and Defence" in *International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014.*

[3] "Network Wrangler - Tech Blog: Why is network security important", https://www.poweradmin.com/blog/why-is-network-security-important/

[4] "Webroot: What is social engineering", http://www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

[5] https://en.wikipedia.org/wiki/Social_engineering_%28security%29

[6] https://en.wikipedia.org/wiki/Computer_security

[7] "The State of Security: 5 social engineering attacks to watch out for", http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[8] The story of HP pretexting scandal with discussion is available at *Davani, Faraz (14 August 2011). "HP Pretexting Scandal by Faraz Davani". Scribd. Retrieved 15 August 2011.*

[9] Fagone, Jason. *"The Serial Swatter". New York Times. Retrieved 25 November 2015.*

[10] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[11] "Open Web Application Security Project (OWASP): Man in the middle attack", https://www.owasp.org/index.php/Man-in-the-middle_attack

[12] "Enterprise Networking Planet: Ways to prevent or mitigate SQL injection attacks", http://www.enterprisenetworkingplanet.com/netsecur/article.php/3866756/10-Ways-to-Prevent-or-Mitigate-SQL-Injection-Attacks.htm

[13] “Open Web Application Security Project (OWASP): Cross-site Scirpting (XSS)”, https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

[14] “CHUBB: Guide to preventing social engineering fraud”, http://www.chubb.com/businesses/csi/chubb19441.pdf

[15] “Microsoft pattern & practices- proven practices for predictable results: Threats and Countermeasures”, https://msdn.microsoft.com/en-us/library/ff648641.aspx

[16] https://en.wikipedia.org/wiki/Email_spoofing