Zoran Cekerevac – Zdenek Dvorak – Ludmila Prigoda – Petar Cekerevac*

TECHNO-ECONOMIC ASPECT OF THE MAN-IN-THE-MIDDLE ATTACKS

This paper analyzes some aspects of the man-in-the-middle (MITM) attacks. After a short introduction, which outlines the essence of this attack, there are presented used scientific methods and hypotheses. The next chapter presents technology of MITM attacks and benefits that a successful attack provides the attacker with. Some of the most significant examples of such attacks, which have a larger scale and significant impact on the broader Internet community, are presented. This part of the article ends with an analysis of possible protection against MITM attacks. Later, on the basis of available data, the analysis of MITM attack from an economic point of view is given. In Conclusion, the summary of the whole analysis is performed.

Keywords: *Man-in-the-middle, IT, Internet, eavesdropping, ARP poisoning, DNS spoofing, SSL hijacking, Internet of things.*

1. Introduction

Every IT expert has heard of the Man-in-the-Middle Attacks (MITM), but this type of attacks is very rarely described in details and well classified. Also, there are rarely shown the benefits the attacker hopes to attain. The aim of this paper is to present an analysis of technology of MITM attacks, their relationship with other types of attacks, and some economic factors in this regard.

In successful MITM attacks an attacker can have the ability to receive data and retransmit it without changing or after changing it, so that results can be the eavesdropping or manipulation.

Every IP implementation must include Internet Control Message Protocol (ICMP). To provide services in the safe way most Internet applications use encrypted connections provided by Secure Sockets Layer and Transport Layer Security protocols on the application layer. Although SSL/TLS can create a two-way trust relationship, because of the complexity in administration, SSL/TLS is mostly used with the one-way trust relationship, which means that only one participant can validate the connection. This method of SSL/TLS application represents a weakness that can be exploited by an attacker.

There are several types of MITM attacks:

- ARP cache poisoning,
- DNS spoofing,
- Session hijacking including side-jacking, evil twin, sniffing, ...
- SSL Hijacking.

Articles about MITM attacks can be found in many sources as, for example: [1 - 6], etc.

In the past, MITM attacks mainly affected laptops, but, now, mass population of cell phone users can be under attack. It is hard to expect that such different crowd can protect itself. Except for standard attacks on IP and data, MITM attacks can target *rel="nofollow"* in the mobile devices, and it can be particularly worrying. A successful attack can allow a hacker to identify a person's location, intercept messages or even eavesdrop on conversations [7].

2. Used scientific methods and hypotheses

Methodological basis of this research includes the principles of the systemic-functional approach to the analysis of phenomena. In justification of theoretical propositions and arguments, following scientific methods were widely used: hypotheticodeductive method, axiomatic method, analytical-deductive method, and comparative method, scientific abstraction, induction and deduction, synthesis,

* [1]Zoran Cekerevac, [2]Zdenek Dvorak, [3]Ludmila Prigoda, [4]Petar Cekerevac
[1]Faculty of Business and Law, "Union - Nikola Tesla" University in Belgrade, Serbia
[2]Faculty of Security Engineering, University of Zilina, Slovakia
[3]Faculty of Economics and Service, Maykop State Technological University, Maykop, Russia
[4]Hilltop Strategic Services, Belgrade, Serbia
E-mail: zoran@cekerevac.eu

comparative analysis, as well as analysis of time series, graphical interpretation etc.

Using basic features, their resolving power, and analytical base of each of the above methods used in accordance with their epistemological potential landmark in the process of solving theoretical and empirical tasks, allowed in the context of a single algorithm to achieve the goal of the article and to provide high representativeness of the results and conclusions.

The null hypothesis was set as:

H_o – *"MITM attacks are extremely rare and make no damages to any user."*

The alternative hypothesis was set as:

H_1 – *"MITM attacks are not extremely rare and can cause losses to victims".*

3. MITM technology

The man-in-the-middle attack, by using different techniques, intends to intercept a communication between two nodes, client, and server. The attacker splits the original TCP connection into 2 new connections. Once the TCP connection is intercepted, the attacker gets the opportunity to read, insert and modify the data in the intercepted communication [5].

An example of the MITM attack is shown in Fig. 1. The attacker interrupted the connection of his victims and usurped the role of a proxy.

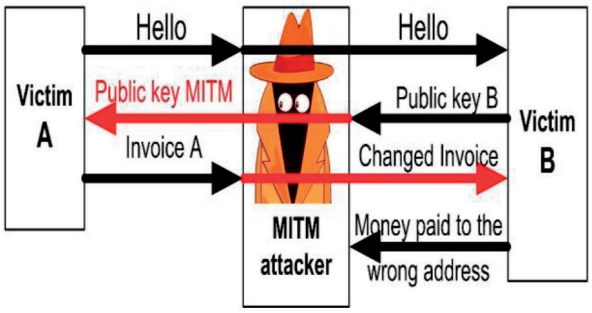

Fig. 1 An example of the MITM attack
Source: Authors based on the [3]

How to conduct a simple man-in-the-middle attack is described in details in the eponymous article [8], therefore, it will not be presented here. After catching the username and the password, the attacker has all that he needs to attack. The attacker can have additional benefits if the victim uses the same username and password for all services and systems.

The main drawback of millions of HTTPS, SSH and VPN servers is that prime numbers generated by Diffie-Hellman key exchange are all the same. With advancements in technology new algorithms appeared, as Field Sieve, which can very efficiently break Diffie-Hellman connections. Nowadays, when two wireless devices share their secret keys by creating a secure channel between them, this is nothing but the Diffie-Hellman exchange [9]. More about scanning for victims, auto detection of local interfaces and default gateways, as well as about the setting up the MITM attacks for the victims, routers, IP forwarding, and restoring the victim after attack was done, can be found in numerous sources, e.g. [10 or 9].

4. Are MITM attacks rare?

Man-in-the-middle attacks existed long before the appearance of computers. One good example might be a malicious postman who opens people's letters and takes or changes their contents before handing over the letter to its recipient. But now man-in-the-middle attacks are essentially eavesdropping and/or manipulating attacks.

According to McAfee research [11] the most frequent are denialofservice and browser attacks. Together, they make 64% of all attacks. They together with SSL attacks constitute the MITM attack. Many protocols that are used every day are vulnerable to various attacks in one way or another, simply because it's quite hard to devise a protocol that's completely secure against MITM. Most solutions are only "best effort", and not "completely and absolutely secure" solutions.

Are the "man in the middle" attacks actually rare in the real world? Data say that MITM is quite credible for concern. The Dutch High Tech Crime Unit's data say that according to their 32 data breach, statistics 15 involved MITM actions [12, p. 69].

In June 2015, 49 persons were busted in Europe for Man-in-the-Middle bank attacks [13]. They were arrested on suspicion of using MITM attacks to sniff out and intercept payment requests from email. This fraud was at the level of €6 million, and was conducted in a "very short time". Targets were medium and large European companies. A similar attack was when crooks were targeting customers of Absa, one of the Big Four banks in South Africa, in 2013. In that case, fraudsters made a fake site looks very professional buyers who will reach it by clicking on a link in a phishing e-mail (a good reason to avoid doing it; instead, type in the URL yourself), asked users to enter their passwords and the Random Verification Number code that Absa sends to mobile phones as a one-time password [13]. The whole scam was carried out with a lot of errors, but it was nevertheless in many cases successful. Although in e-banking some of the controls brought in by banks (two-factor authentication etc.) were applied to combat the attacks on customers, this case shows that they are not always sufficient.

There are, also, many other ways to attack e-banking users as the use of malware to place a Trojan on the client PC, but MITM is still relatively easy in most cases. The main reasons for MITM attacks are:

– low risks - physical and to be caught,

– some effort in coding the exploit can lead to real world monetary gain, and
– the code can then be reused or sold to other criminals.

It seems that the larger problem is how to wash the stolen money and not to be detected than to reveal the fraud.

However, the theft of money is not always the goal of the scam. Some say that "...employer does an MITM attack on us. They use it in order to monitor our email and prevent us from sending attachments" [14]. Michael Hex [15] claims that MITM attacks within companies happen daily and more than once. Others think that MITM attacks are "common enough to be an official government policy" [16].

One of the most interesting incidents happened in the year 2008. FARC (Revolutionary Armed Forces of Colombia) was attacked by series of DoS and MITM attacks in order to free up 15 hostages. These attacks freed them without a single ammunition being involved [17].

One of the first, well-known MITM attacks was the Mitnick attack. To take over a session Mitnick exploited the basic design of the TCP/IP protocol. The attack was performed through:

– identifying weaknesses of the network and collecting the necessary information,
– silencing the actual network server and replacing it with own computer, and
– hijacking.

Mitnick's attack to Shimomura's computer is in details described in [18]. An identical attack is nowadays impossible because we don't use *rsh*; but we use SSH [19].

Nowadays many other possible scenarios can exist:

– command injection; useful where one-time authentication is used,
– malicious code injection; malicious code insertion into an email or web pages,
– key exchanging; public key exchanged by server and client modification,
– parameters and banners substitution; Parameters exchanged by server and client can be substituted in the beginning of a connection. For example, the attacker can force the client to initialize an SSH1 connection instead of the SSH2,
– IPSEC failure; Block the key material exchanged on the port 500 UDP. If the client is configured in rollback mode, there is a good chance that the user will not notice that the connection is in clear text,
– PPTP attacks; The Point-to-Point Tunneling Protocol as the method for implementing VPNs has many known security issues,
– Transparent proxy; The attacker adds his own URL in the front when the victim loads the URL of a defaced web page.

More details about mentioned scenarios can be found in [20 - 21].

One attack of enormous size using MITM technology was performed by the NSA in 2013. Tor was attacked to be compromised. Previous attacks failed to directly break Tor, but this attack was more successful by using vulnerabilities in Firefox to target certain Tor users. The attack was possible because of the major telcos letting the NSA put servers directly off the backbone. More detailed explanation of this attack can be found in [22].

One of the recent man-in-the-middle attacks was in July 2015 hacking a Jeep Cherokee, which caused a major recall by Chrysler Corporation. Without important security safeguards being put in place and rigorously tested, hackers can eventually control the vehicles' basic functions, such as brakes, steering, and acceleration which could be highly dangerous [23]. A modern car may be connected to multiple networks including cellular, V2V/V2I/V2X, Bluetooth, Wi-Fi and Wired Automotive Ethernet, and this appears as an added risk. Many people still don't realize, but beside the TVs, the IoT will soon involve many devices as washing machines, refrigerators, etc. Each home device will have an IP address and therefore, will be vulnerable to attacks.

In March 26, 2016, GitHub experienced the largest DDoS (distributed denial of service) attack in its history. The attack involved a wide combination of attack vectors. These included every vector they had seen in previous attacks as well as some sophisticated new techniques that used the web browsers of unsuspecting, uninvolved people to flood github.com with high levels of traffic [24]. Netresec made a deeper analysis of this attack and concluded that China was using their active and passive network infrastructures in order to perform a packet injection attack, known as a man-on-the-side attack against GitHub [25]. The man-on-the-side attack is similar to MITM attack, with similar technology, but with less controlling of a network node.

In October 21, 2016, a series of DDoS attacks caused rough disruption of legitimate internet activity in the US. The attacks targeted the Domain Name System and were perpetrated by directing huge amounts of bogus traffic at targeted servers belonging to Dyn which is a major provider of DNS services to other companies. A lot of activities such as online shopping, social media interaction, etc., were not possible to use for some periods of time. The length of disruptions varied, but in some cases, it took several hours. Detailed information about October 21 attack can be found in [26].

And finally, the answer to: "Are MITM attacks rare?" is No! Some, more stringent, analysts say that any instance of an SSL root getting a bad cert can consider it as a sign of an attack. One should always bear in mind that MITM can be part of a denial-of-service attack [27].

5. How to confront MITM attacks?

Michael Gregg [28] named six ways how one can become a victim of MITM attack:

- Wi-Fi Eavesdropping,
- Man-in-the-browser,
- Man-in-the-mobile,
- Man-in-the app,
- Man-in-the-cloud, and
- Man-in-the-IoT.

It is a great variety of possible attacks. Complete elimination of MITM attack is a very difficult task, but the careful user can significantly reduce the risk.

Several security vendors have solutions to scan encrypted traffic (for example, Palo Alto Networks, Kaspersky Internet Security 2015, etc.) and the companies can activate this feature. To do this, the firewall/proxy device is simply granted a certificate from internal Certificate Authority (CA) which is already trusted by all clients. When an application asks for a secure connection, the firewall/proxy device generates a new certificate for the target server on the fly and sent it to the client. Since the client trusts the internal CA, it also trusts the device certificate and will happily start a "secure" connection.

MITM attacks are the preferred choice of attack for surveillance groups who want to sniff on the data on a connection [9]. From defender´s point of view, ARP cache poisoning happens in the background with very few chances to be controlled by the user. Although difficult, some of the countermeasures can be adopted to provide a shield. There is no catch-all solution, but proactive and reactive measures can be taken.

New patched and updated operating systems must be used on a network. Also, security of network should be the primary concern while designing it [9]. If the network configuration is not changing frequently, it is quite feasible to make a listing of static ARP entries and deploy them to clients via an automated script. This can ensure that devices rely on their local ARP cache rather than relying on ARP requests and replies [6]. This way the process is little less dynamic.

DNS spoofing is mostly passive by its nature so it is difficult to defend. Users never know that their DNS is being spoofed until it has happened. In very targeted attacks it is possible that the user may never know that he has been tricked into entering his credentials into a false site until he receives a bill from his bank. But, there are still a few things that can be done to defend against these types of attacks [29]:

- internal machines securing,
- not to rely on DNS for secure systems,
- use of IDS, and
- use of DNSSEC.

Unless the attacker makes some of the obvious action when he hijacks a session, one may never know that an attacker was there. A few things can be done to better defend against session hijacking [30]:

- to do online banking from home,
- to be cognizant and keep an eye out for things that seem unusual, and
- to secure own internal machines; such attacks are mostly executed from inside the network.

SSL hijacking is virtually undetectable from the server side because for the server the communication with a client is quite normal. He can't see that he communicates with a proxy. Some things can be done from the client's side [31]:

- to ensure secure connections using HTTPS,
- to do online banking from home, and
- to secure own internal machines.

6. The Economic Aspect

It is rather rare to find real world data on MITM attacks. One of the reasons is that MITM attacks are by their nature usually targeted at individuals. On the other hand, "a lot of the attacks you hear about are just the tip of the iceberg. Banks often won't even tell an affected customer that they have been a victim of these man-in-the-middle attacks" [32]. Franklin also said: " 'man-in-the-browser' attacks are emerging to compete in popularity with middleman threat", and that (in Europe, Middle East and Africa, in 2007) "3.5 million adults remembered revealing sensitive personal or financial information to a phisher, while 2.3 million said that they had lost money because of phishing. The average loss is US$1,250 per victim".

The situation with defining costs caused by MITM attacks is more complicated when we know that, as mentioned earlier, MITM attacks are closely connected with the major attacks, including DDoS.

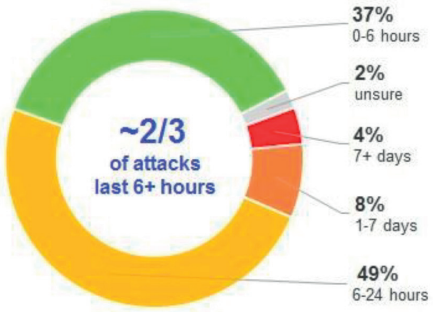

Fig. 2 The average attack length
Source: Authors based on [34]

Analyzing a DDoS attack in October 21, 2016, Lafrance [33] claimed that in the year 2014 "For more than one-third of companies, a single hour of a DDoS attack can cost up to

$20,000". Matthews [34], upon an examination, concluded that "the data reveals there are no predictable patterns as to how long an assault will last". Some statistics is given in Fig. 2. It is easy to multiply cost for an hour by the number of hours and the number of attacks. For some companies, it can reach millions. "The airline Virgin Blue lost $20 million in a period of IT outages that spanned 11 days in 2010" [33].

Per Ponemon global study and research of 2016 cost of data breach [35] that covered 383 companies, the average total cost was increased from $3.79 (in 2015) to $4 million (in 2016). The average cost of stolen or lost record containing sensitive information was increased from $154 (in 2015) to $158 (in 2016). Comparing to 2013 total cost of a data breach is increased or 29%, or 15% per capita. It is interesting that risks from a data breach are not evenly distributed. Organizations in Brazil and South Africa are much more exposed to material data breaches then organizations in Germany and Australia.

The Ponemon analysis showed that a cost per compromised record, or per capita, in average is on the level of $158. The highest values are in healthcare organizations with $335, then in education ($246), transportation ($129), research ($112), and public sector ($80). The most data breaches were caused by hackers and criminal insiders. The analysis showed that 48% were caused by criminal attacks. The average cost of attacks resolving was $170, while costs of system glitches and human errors were $138 and $133 respectively. The most expensive resolving of attacks was in the US ($236), and the cheapest was in India ($76 per record).

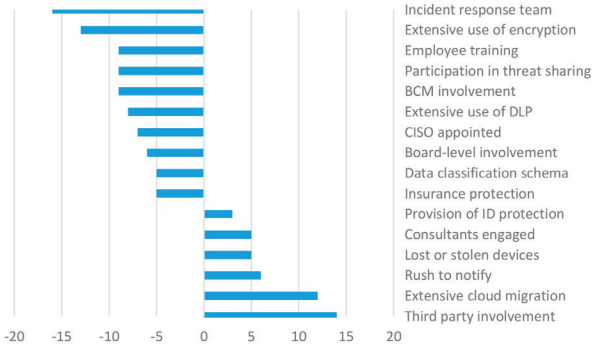

Fig. 3 Impact of 16 factors on the per capita cost of data breach [35]

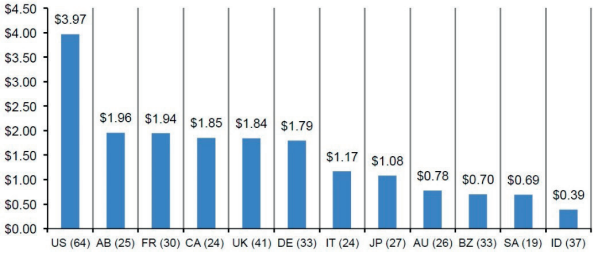

Fig. 4 Lost business costs for 383 companies in US$ million
Source: [35]

Fig. 3 shows the actors that influence the cost of incident resolving. The third-party involvement caused an increase of $14.

Carried out attacks that prevent companies from doing business on the Internet mostly affect those companies that are more oriented to the Internet and especially companies that operate in the most developed countries. The costs of business losses were particularly high in the case of US companies, as shown in Fig. 4.

These losses include reputation losses, goodwill diminishing, increasing of customer acquisition activities, and the abnormal turnover of customers.

7. Conclusions

Theft and eavesdropping have existed since the beginning of time. Today they are largely migrating to the Internet. The struggle is constant and the attackers usually take advantage of both in terms of knowledge and technology at their disposal. MITM attacks, despite some limitations, remain effective technology for carrying out attacks and acquiring illegal benefits. They are performed in different versions, but with the same basic idea. An MITM is often combined with other attacks or built into them.

MITM attacks are usually performed in order to acquire some benefit, financial or non-financial. In cases where private individuals were attacked, the attacks often remain undiscovered and statistically unrecorded. In the cases of attacks on economic operators the attacks often remain hidden to public to preserve the company's image, so in these cases it is also difficult to accurately assess the consequences. Only in cases of large-scale attacks, when they hit a lot of Internet users the extent of the damage caused comes to light.

Despite difficulties in collecting relevant data, this analysis on some examples showed the extent of the damage that can be caused by MITM attacks. Also, the analysis showed that the most vulnerable are mobile devices and Wi-Fi data transmission and that the biggest threat to users is when they are connected to the Internet via a public Wi-Fi connection.

It is not possible to provide a protection that would be effective in all circumstances and in all situations, but for all users, a good idea is not to use public Wi-Fi in situations when doing anything sensitive and/or confidential.

Analysis showed the great potential of IoT, but also the risks that may occur from insufficient protection.

Finally, the research showed that the null hypothesis H_0 is rejected. The research showed that the MITM threat is real, and that can bring significant losses to victims. That way the alternative hypothesis H_1 is proven.

References

[1] PRIGODA, L., et al.: *One Look at the Modern Information Security.* Sustainable Development of Mountain Territories, vol. 4, No. 22, Apr 19, 2015.

[2] CEKEREVAC, Z., DVORAK, Z., CEKEREVAC, P.: *Internet Safety of SMEs and E-mail Protection in the Light of Recent Revelations about Espionage of Internet Communication System.* Chernivtsi : Bukovina University, Zbirnyk naukovykh prats' Bukovyns'koho universytetu. Ekonomichni nauky, vol. 10, 2014, 2219-5378.

[3] DuPAUL, N.: Man in the Middle (MITM) Attack. *Veracode.* [Online] [Cited: Nov 28, 2016.] http://www.veracode.com/security/man-middle-attack.

[4] GANGAN, S.: *A Review of Man-in-the-Middle Attacks*. *arXivorg.* [Na mrezi] 2015. https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf.

[5] OWASP.: *Man-in-the-middle Attack*. *OWASP.* [Online] Aug 31, 2015. https://www.owasp.org/index.php/Man-in-the-middle_attack.

[6] SANDERS, C.: Understanding Man-in-the-Middle Attacks - ARP Cache Poisoning, Part 1, *Windowsecurity.* [Online] Mar 17, 2010. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html.

[7] COVINGTON, M.: Free Wi-Fi and the dangers of mobile Man-in-the-Middle attacks, *Betanews.* [Online] Oct 8, 2016. http://betanews.com/2016/10/08/free-wi-fi-mobile-man-in-the-middle-attacks/.

[8] –. How to Conduct a Simple Man-in-the-middle Attack, *Wonderhowto.* [Online] 2014. http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/.

[9] KAPIL, J., MANOJ, J. and BORADE, J.: *A Survey on Man in the Middle Attack. IJSTE*, vol. 2, No. 9, 2016, pp. 277-280.

[10] EDWARDS, R.: Simple Man-in-the-Middle Script: For Script Kiddies. *Wonderhowto.* [Online] Aug 119, 2016. http://null-byte.wonderhowto.com/news/simple-man-middle-script-for-script-kiddies-0168192/.

[11] McAFEE.: *McAfee Labs Threats Report, September 2016.* CA: Santa Clara: Intel Security, 2016.

[12] BAKER, W., et al.: *2011 Data Breach Investigations Report, Part*. l, Verizon, 2011. p. 74.

[13] VAAS, L.: 49 Busted in Europe for Man-in-the-Middle Bank Attacks. *Naked Security.* [Online] Jun 11, 2015. https://nakedsecurity.sophos.com/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/.

[14] USER606723.: Are "man in the middle" attacks extremely rare? *Information Security.* [Online] Feb 22, 2012. http://security.stackexchange.com/questions/12041/are-man-in-the-middle-attacks-extremely-rare.

[15] HEX, M.: Are "Man in the Middle" Attacks Extremely Rare? *Information Security.* [Online] Feb 22, 2012. http://security.stackexchange.com/questions/12041/are-man-in-the-middle-attacks-extremely-rare.

[16] JUPP0R.: Are "Man in the Middle" Attacks Extremely Rare? *Information Security.* [Online] Feb 22, 2012. http://security.stackexchange.com/questions/12041/are-man-in-the-middle-attacks-extremely-rare.

[17] VIECCO, C, CAMP, J.: *A Life or Death InfoSec Subversion.* 5, 2008, Security & Privacy, Vol. 6, pp. 74-76.

[18] ERIKSSON, M.: *An Example of a Man-In-The-Middle Attack Against Server Authenticated SSL-sessions.* Stockholm: Simovits Consulting, 2016.

[19] SUNDARAM, R.: The Kevin Mitnick Attack. *Northeastern University.* [Online] Feb 16, 2011. http://www.ccs.neu.edu/course/cs6740/Lectures/Lecture-7.pdf.

[20] ORNAGHI, A., VALLERI, M.: *Man in the Middle Attacks.* Amsterdam: BlackHat, 2003. Blackhat Conference. p. 61.

[21] ORBITCO.: What is Man in the Middle Attacks ? Explained with Examples, *Orbit-computer-solutions.* [Online] Nov 9, 2015. http://www.orbit-computer-solutions.com/network-attack-man-in-the-middle-attacks/.

[22] SCHNEIER, B.: Attacking Tor: How the NSA Targets users' online Anonymity . *The Guardian.* [Online] Oct 4, 2013. https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

[23] SIMKO, C.: Man-in-the-Middle Attacks in the IoT. *GlobalSign.* [Online] Feb 26, 2016. https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/.

[24] NEWLAND, J.: Large Scale DDoS Attack on github.com. *github.* [Online] Mar 27, 2015. https://github.com/blog/1981-large-scale-ddos-attack-on-github-com.

[25] –. China's Man-on-the-Side Attack on GitHub. *Netresec.* [Online] Mar 31, 2015. http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub.

[26] COB, S.: 10 things to know about the October 21 IoT DDoS attacks, *Welivesecurity.* [Online] Oct 24, 2016. http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/.

[27] CISCO: Threats in Borderless Networks. *LearnCisco.* [Online] n.d. http://www.learncisco.net/courses/iins/common-security-threats/threats-in-borderless-networks.html.

[28] GREGG, M.: Six Ways You Could Become a Victim of Man-in-the-middle (MiTM) Attacks this Holiday Season. *The Huffington Post.* [Online] 12 11, 2015. http://www.huffingtonpost.com/michael-gregg/six-ways-you-could-become_b_8545674.html.

[29] SANDERS, C.: Understanding Man-In-The-Middle Attacks, Part 2: DNS Spoofing, *Windowsecurity.* [Online] Apr 7, 2010A. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html.

[30] –. Understanding Man-In-The-Middle Attacks, Part 3: Session Hijacking, *Windowsecurity.* [Online] May 05, 2010B. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html.

[31] –. Understanding Man-In-The-Middle Attacks, Part 4: SSL Hijacking. *WindowSecurity.* [Online] Jun 9, 2010C. http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html.

[32] FRANKLIN, D.: Threatwatch: How much to MITM, how Quickly, how much Lost. *Financial Criptography.* [Online] July 23, 2007. http://financialcryptography.com/mt/archives/000941.html.

[33] LAFRANCE, A.: How Much Will Today's Internet Outage Cost? *The Atlantic.* [Online] Oct 21, 2016. http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/.

[34] MATTHEWS, T.: Incapsula Survey: What DDoS Attacks Really Cost Business, *Incapsula.* [Online] 2014. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf.

[35] PONEMON.: *IBM - 2016 Cost of Data Breach Study: Global Analysis,* US-MI: Traverse City : Ponemon Institute, 2016. p. 32.