MEST JOURNAL
DOI 10.12709/mest.05.05.02.03

INTERNET OF THINGS AND THE MAN-IN-THE-MIDDLE ATTACKS – SECURITY AND ECONOMIC RISKS

Zoran Cekerevac
Faculty of Business and Law, "Union - Nikola Tesla" University in Belgrade, Republic of Serbia

Zdenek Dvorak
Faculty of Security Engineering, University in Zilina, Slovak Republic

Ludmila Prigoda
Faculty of Economics and Service, Maykop State Technological University, Maykop, Russia

Petar Cekerevac
Hilltop Strategic Services, Belgrade, Republic of Serbia

JEL Category: **G32, M15**

Abstract

This paper presents some aspects of the Internet of Things (IoT) and attacks to which IoT may be exposed, above all, the man-in-the-middle (MITM) attack. After a short introduction, which describes the essence of the IoT and the MITM attack, scientific methods used, and hypotheses are presented. The next chapters show the technology of MITM attacks and the benefits that a successful attack provides to attackers. Here are presented also some of the most important examples of such attacks, which had a wider scope or significant impact on the Internet community. This part of the article ends by analyzing the possibilities of protection of IoT against MITM attacks. In the continuation, based on the data available, an analysis of MITM attacks is given from an economic point of view. The conclusions show a summary of the entire analysis with assumptions of the future development of these issues.

Keywords: *Communication systems, computer networks, Computer applications*

1 INTRODUCTION

The Internet of Things (IoT), a system of interrelated computing devices, with its rapid development and distribution, came into the focus of interest of Internet users, especially the users of smart devices. This is supported by the fact that the IoT is not limited to mechanical and digital machines, but also covers other objects, animals, and even people that are provided with unique identifiers that can transfer data over a network. Because of this, nowadays, it is often used as a

Address of the corresponding author:
Zoran Cekerevac
zoran@cekerevac.eu

term with the broadest meaning, the Internet of Everything. During this interaction, any human activity is not required.

In his work, Evans (2011) predicted that in the year 2020, there will be 50 billion devices connected to the Internet. Good visualization of Internet development is shown in (Cisco, 2016) Thus, the massive deployment of IoT will cause a greater difference between the current understanding of the Internet, which came down to the "dot-com", "social" or "experience" web, and new evolution of the Internet that will lead to new and revolutionary applications with potential to significantly improve the quality of life. They will change the way people live, learn, work, and entertain themselves (Evans, 2011).

It is nice and useful when smart devices like TVs or watches are connected to the Internet and receive, or send, the data that the user wishes. But, before reaching their final destinations data pass through all four steps of the TCP/IP model, and they are exposed to all well-known risks. With extensive use of Cloud storage, it can be said that there is a fifth layer, the Cloud layer. The possibility of this layer being attacked is high, starting with brute force attacks at password-based attacks. Also, it is possible to change data at the Session layer using Man-in-the-Middle (MITM) attacks. One should not lose sight of sniffer attacks, denial of service (DoS), as well as compromised-key attacks.

Every IT expert has heard of the Man-in-the-Middle attacks, and this type of attacks is frequently described in different articles. Together with the networking technology growth, cloud computing, the Internet of Things (IoT), and Bring Your Own Technology (BYOT), attackers are finding new ways to make MITM attacks attractive again. This paper aims to present a brief analysis of the technology of MITM attacks together with some examples of attacks of this kind, and some economic factors in this regard.

2 USED SCIENTIFIC METHODS AND HYPOTHESES

The methodological basis of this research includes the principles of the systemic-functional approach to the analysis of phenomena. In justification of theoretical propositions and findings, there were widely used the following scientific methods: hypotheticodeductive method, axiomatic method, analytical-deductive method, comparative method, scientific abstraction, induction and deduction, synthesis, and comparative analysis, as well as analysis of time series, graphical interpretation, etc.

The null hypothesis was set as:

H_o – "MITM attack is an old technology and can't cause damages to the attacked in the IoT."

The alternative hypothesis was set as:

H_1 – "MITM attacks are not rare in the IoT and can cause losses to the victims".

3 MITM TECHNOLOGY

Man-in-the-middle attacks existed long before the appearance of computers. To show the basics of the MITM attacks it can be used the example of a malicious postman who opens people's letters and reads or changes their contents before handing over the letter to its recipient.

Most Internet applications strive to use encrypted connections provided by SSL/TLS protocols on the application layer to provide services in a safe way. SSL/TLS can create a two-way trust relationship, but because of the complexity of administration, SSL/TLS is mostly used when only one participant validates the connection. This method represents a weakness, which can be exploited to attack.

The man-in-the-middle attack, using different techniques, intends to intercept a communication between two nodes. Once the attacker interrupts the connection of his victims, he can usurp the role of a proxy. An example of the MITM attack is shown in Figure 1. To send an invoice to user B in a "safe" way user A wishes to encrypt the message. He sends "Hello" and asks for B's public key. MITM attacker forwards the message and follows the reaction of B. Upon receiving B's public key, the attacker keeps it and sends his own public key to his victim A. Believing that he has received the real B's key, user A encrypts the invoice and sends it to B. The attacker receives the A's invoice and because the invoice was encrypted with the attacker's key, he can read it. In the message, the attacker changes elements of the payment and the new changed encrypted invoice he sends to victim B. Believing that he has received the requested invoice B pays the money to the wrong bank account and starts to wait for paid goods.

The attacker takes the deposited funds, disappears, and leaves victims to litigate themselves. This type of attack is called manipulation. The attacks in which messages are only read and forwarded unchanged belong to another group of MITM attacks, eavesdropping.

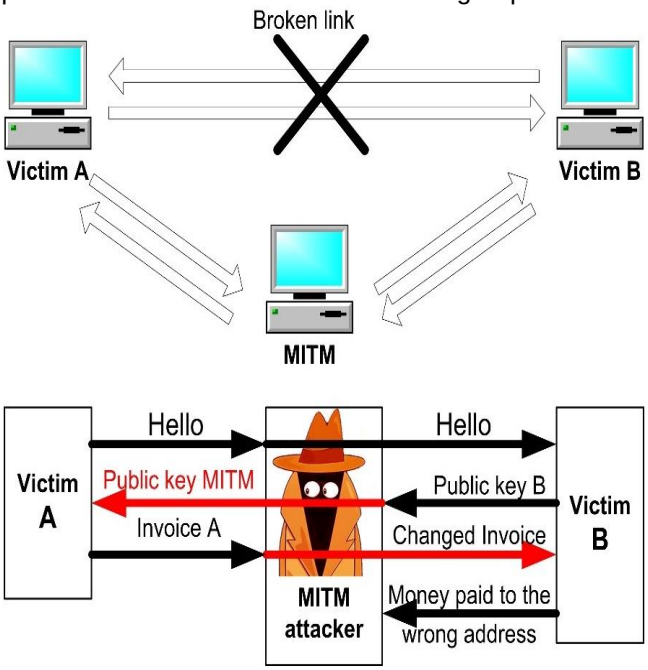

Figure 1 An example of the MITM attack

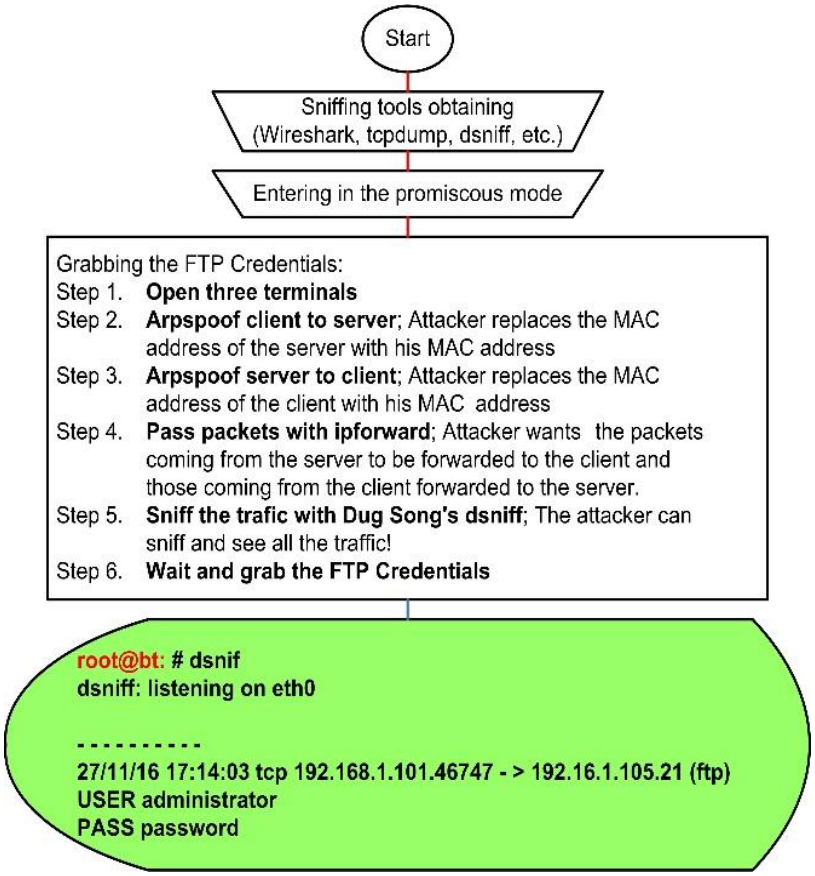

Figure 1. Sniffing and the FTP credentials grabbing
Authors visualization of (How to conduct a simple man-in-the-middle attack, 2014)

MITM attacks can be conducted in several ways:

- Address Resolution Protocol (ARP) cache poisoning,
- DNS spoofing,
- Session hijacking including side-jacking, evil twin, sniffing,
- SSL Hijacking.

These methods are well explained in the literature and will not be herein discussed in detail. An algorithm of the FTP credentials grabbing is presented in Figure 2.

The example shown in Figure 2 illustrates the dsniff application to collect text data on unsecured connections, which is its primary function. Dsniff is a network sniffer, and it sniffs cleartext usernames and passwords, web pages being visited, contents of emails, etc. After catching the username and the password, the attacker has all that he needs to attack. The attacker can have additional benefits if the administrator uses the same username and password for all services and systems.

In the past, MITM attacks mainly affected laptops, but now, thanks to a mass population of cell phones great number of users can be under attack. The problem might be even worse because a recent Symantec study showed that around 50% of respondents did not even think about their data protection. (Covington, 2016).

The introduction of computers in numerous devices, their networking, and their connection to the Internet further increase the number of potential endangerments. It is interesting to see how these attacks can be carried out in the IoT.

One of the first ways is the local attack via Ethernet connection or Wi-Fi. An attacker with access to the local home network can perform attacks against smart home devices on two common modes: cloud polling and direct connection.

In the first case, in the cloud polling, the smart home device is in constant communication with the cloud. The smart device uses this method when wants to continuously check the cloud server whether there is a new firmware version available. If yes, it uploads its status. To target such an application, attackers can perform an MITM attack. They can redirect network traffic using ARP poisoning or by DNS settings modifying. To intercept HTTPS traffic attackers can use a self-signed certificate or some tools such as SSLstrip. When the connection is done over HTTPS, some of the smart devices do not verify whether the certificate is trusted. Per (Barcena & Wueest, 2015), “none of the tested devices perform a mutual SSL authentication, where both sides authenticate with one another instead of just the server authenticating with the client. Most devices completely ignore certificate revocation lists, allowing an attacker to use keys that were obtained through a data breach without any problem”.

In the case of direct connections, devices communicate with a hub or application in the same network. This way, a mobile app can locate new devices by scanning and probing every IP address on the local network for a specific port. The Simple Service Discovery Protocol and the Universal Plug and Play (SSDP/UPnP) protocols can be used to discover the devices. Any attacker can do the same.

About scanning for victims, auto-detection of local interfaces and default gateways, as well as about setting up the MITM attacks for the victims, routers, IP forwarding, and restoring the victim after the attack was done, can be found in numerous sources, e.g. (Edwards, 2016) or (Kapil, Manoj, & Borade, 2016), and will not be further analyzed here.

There are a variety of tools available to conduct a man-in-the-middle attack. Here are some of the tools that can be used for network and host analysis, but which also have MITM attack capability.

- Ettercap – a comprehensive suite for MITM attacks. It features sniffing of live connections, content filtering on the fly, and many other options. “It includes many features for network and host analysis and supports the dissection of many protocols.” (Ornaghi & Valleri, 2015)
- evilgrade – a modular framework that allows taking advantage of poor update implementations by injecting fake updates and making hostname redirections (manipulation of victim’s DNS traffic). (Amato & Kirschbaum, 2010) (Jamie, 2016)
- SSLstrip – a tool that transparently hijacks HTTP traffic on a network, watches for HTTPS links and redirects, and then maps those links

into look-alike HTTP links or homograph-similar HTTPS links. It also supports supplying a favicon which looks like a lock icon, selective logging, and session denial. (Marlinspike, 2014) Shortly, turns https:// URLs into http:// URLs.

- Dsniff – Per Song (2001) "dsniff is a collection of tools for network auditing and penetration testing. *Sshmitm* and *webmitm* implement active man-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI."
- Cain and Abel, a Windows-based password recovery tool – Per Montro, this tool allows the use of sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. Using it, it is easy to recover various kinds of passwords. (Montoro, 2014)

Smart devices, and consequently IoT, can be also endangered through Bluetooth hacks. Bluetooth Low Energy is probably the most thriving IoT technology and can be used for many applications, e.g., for sensors, home automation, household goods, medical devices, door locks, alarms, banking tokens, and smart every-things. Bluetooth Low Energy (BTLE, or BLE), a.k.a. Bluetooth Smart is a new mode of modulation and link layer packet format for low-energy Bluetooth applications. It was defined in the Bluetooth Core Spec 4.0. (Marquess & et al., 2010)

Some can say that the Bluetooth operating range is limited and that an MITM attack can be difficult to perform because an attacker must be close to both attacked devices. But, BLE can have a range of more than 100 m. Furthermore, in some cases, the devices even do not need to be close to each other. The attacker can relay packets remotely, via the Internet.

Some mobile applications possess proximity features that might be abused by approaching the smartphone running the affected application away from the device and its original location. Mobile malware may attack BLE devices in the range of the infected smartphone. Such malware is operated remotely, and the attack is theoretically possible on a mass scale. (Jasek S. , 2016)

In his research, Slawomir Jasek (2016) found that the growing number of Bluetooth devices used for keyless entry and mobile point-of-sales systems were vulnerable to MITM attacks. He noted that, although the BLE specification provides secure connections through link-layer encryption, device whitelisting, and bonding, "companies too often do not implement correctly that protections, and this lack could allow attackers to clone BLE devices." After cloning, the attackers "can gain unauthorized access to physical devices when a smartphone is used as a device controller", as well as capture and manipulate data transferred between the two BLEs. "Jasek estimates that 80 percent of BLE smart devices are vulnerable to MITM attacks. (Spring, 2016)" Per this research, 80% of reviewed devices were incorrectly configured allowing hackers to use some hackers' tools, such as GATTacker, to perform an MITM attack. Jasek explained that by using a few simple tricks, one can ensure that the victim will connect to the attacker's impersonator device instead of the original one. "Common flaws possible to exploit, including improper authentication, static passwords, not-so-random PRNG, excessive services, and bad assumptions" – allow to attacker "to take over control of smart locks and disrupt a smart home (Spring, 2016)".

It is interesting how MITM attacks have adopted themselves in nowadays circumstances. Here are some new experiences.

3.1 MIT-cloud (MITC)

Cloud computing has become a standard service for many companies. For most of them, using cloud-based storage is a very acceptable solution. Storage capacities are large enough to accept large amounts of data that can be transferred easily. It is easy to understand that these services will not demand user log on with his strong passwords for each data transmission session. It would be very uncomfortable for users, and many of these services, after the first authentication, use a session token saved on the user's local system. If an attacker can steal the token, he would have full control over the account, and he can do whatever he wants. One of the possibilities is that the attacker infects the user's computer by uploading malware.

3.2 MIT-browser (MITB)

A lot of people use (and will use) e-banking. The idea of MITB attacks is that an attacker in some way inserts a Trojan into the victim's computer. After that, the Trojan will be waiting for the user to visit the targeted banking website. When the victim attempts to visit the targeted URL, the malware injects special HTML code into the original web page code, which may trick the user. If the user is not well educated and extremely careful, he will not notice small differences between the current and original user interface. After that, "banking services" will be "provided" by the attacker.

3.3 MIT-mobile (MITMO)

Although it is not as safe and comfortable as the use of desktop computers or laptops, many users prefer to make their financial transactions over their smartphones. Therefore, an MITMO deserves increased attention. This type of attack is focused on mobile transaction authentication numbers (mTANs) and transaction authentication codes. This attack intercepts SMS traffic and forwards the captured codes to the attacker. The MiTMO presents a real and great challenge for out-of-band authentication systems. (Gregg, How new technologies are reshaping MiTM attacks, 2015)

3.4 MIT-app (MITA)

MITA attack can be conducted when an application does not perform certificate validation properly. In MITA attacks, an attacker, before starting communication with the application, successfully inserts a self-signed certificate. He exploits how the applications handle trust. The hacker can then intercept application data, steal information, or impersonate the victim on the application. (Gregg, 2015)

3.5 MIT-IoT

With the increasing adoption of IoT, MITM attacks will become a bigger and bigger challenge. One type of MIT-IoT attacks targeted on smartphones, and caused by poor validation of certificates was already discussed in MITA. But, another example, more closely to home devices, could be IoT refrigerators that display a user's Google calendar. It was found that they did not validate SSL certificates. This slip could result in the mounting of an MITM attack and the stealing of the user's Google credentials. (Gregg, How new technologies are reshaping MiTM attacks, 2015)

4 ARE THE MITM ATTACKS RARE IN THE IOT?

According to McAfee research (McAfee, 2016), the most frequent attacks are DoS and MITB attacks (Fig. 3) and they together with SSL attacks constitute the MITM attack. Together they make 64% of all attacks.

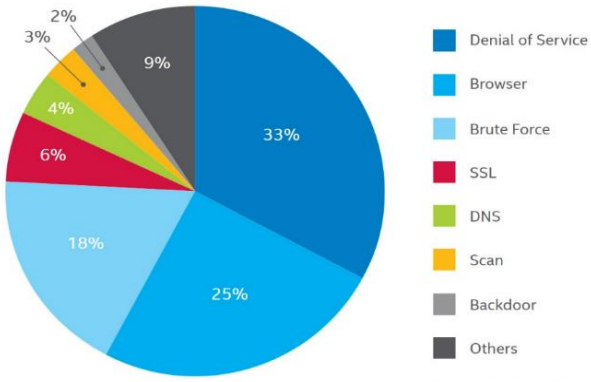

Figure 2. Top network attacks

Source: (Song, 2001)

There are billions of vulnerable IoT devices, and their number is growing rapidly. Most of them are always turned on and reside on unmonitored networks. If these networks allow high-speed connections, a compromised device can be a source of large DDoS attack traffic. So, embedded Internet-of-Thing (IoT) botnets are our present and future. They already were used for DDoS attacks, spam sending, MITM credentials hijacking, Internet chaos making, and other malicious activities. One of the massive attacks with involving compromised IoT devices against dynamic domain name service provider Dyn is analyzed in (Gallagher, 2016) Here, however, we will not thoroughly deal with DDoS attacks. Here will be considered mostly risks connected with devices like cars, webcams, DVRs, cable television, and satellite set-top boxes, etc.

Embedded IoT devices are often maintenance-free and with low-interaction-level. Therefore, frequently, end-users are not aware of possible attacks. Barcena and Wueest, in their research (2015) by analyzing the network traffic, noticed that "the LightwaveRF smart hub generates certain network traffic each time it restarts and every 15 minutes to check for firmware updates".

The device sent traffic to a remote TFTP server on the Internet. Since the TFTP protocol is a very basic file transfer protocol, this connection is not encrypted and authenticated. Therefore, it can be subject to MITM attack.

In the summer of 2014, Samsung brought out their RF28HMELBSR smart fridge. The fridge implements SSL, but it failed to validate SSL certificates. This way it enabled man-in-the-middle attacks against other connections including those made to download Gmail calendar information for the on-screen display. Using MITM it is possible to steal a victim's Google credentials. According to (Venda, 2015), the exception is when the terminal connects to the update server. During the testing of security, it was possible to isolate the URL https://www.samsungotn.net. This URL is also used by TVs, etc., but communications between the fridge terminal and the update server couldn't be intercepted.

Other devices connected to IoT also can be victims of MITM attacks. It is easy to imagine a scenario where a malicious competitor may want to fake temperature data from a monitored device, change them, and forward them to the monitoring equipment. Getting false data, the heat controller can cause machinery to overheat and consequently cease production. Besides stopping production, this can also cause physical and financial damage to the operating organization. (Simko, 2016)

One of the reasons why IoT devices are attractive to attackers is that many of these devices are delivered with insecure defaults. It includes (Arbor, 2016):

- default administrative credentials.
- open access to management systems via the Internet-facing interfaces on these devices.
- shipping with insecure, remotely exploitable code,
- embedded systems that are rarely, if ever, updated, and
- a lack of security updates. Many vendors make no updates at all.

Modern connected vehicles may be connected to multiple networks including cellular, Bluetooth, Wi-Fi, and Wired Automotive Ethernet. These advantages appear as an added risk. One of the recent man-in-the-middle attacks on smart motor vehicles was the July 2015 hacking of a Jeep Cherokee. Without the use of important security measures, hackers can be able to control the vehicles' basic functions, such as brakes, steering, and acceleration, which could be highly dangerous. (Simko, 2016)

And finally, are MITM attacks rare in the IoT? No! Some analysts say that any instance of an SSL root getting a bad cert can consider it a sign of an attack. (Cisco, Threats in Borderless Networks, n.d.)

5 HOW CAN IOT CONFRONT MITM ATTACKS?

As shown, there is a great variety of possible MITM attacks. Their complete elimination is a very difficult task, but the careful user can significantly reduce the risk. Because of the great scope of features that each computer owns, there are very different types of MITM attacks, but also different types of defenses that can be applied. Although there is no magic wand that can protect a computer from all attacks, one of the best approaches is to think about the protection already at the phase of creating the network, and then to update the operating system patches regularly. IoT devices are unique and made for specific purposes, and therefore their protection is specific and, to some extent, can be easier. However, the number and diversity of devices, and the strive for cheaper solutions are also aggravating factors. These devices are frequently released with security vulnerabilities, and they can be prone to MITM attacks.

In stable devices, which are located within a secure private network, the first line of defense is at the router level, and the second at the level of the device. Given the fact that the devices are constantly connected to the Internet, that each device has its original software, and that is rarely monitored by a user, possible protection comes down to a proper firewall configuration and periodical (regular) updating of software from trustworthy sources. Where it is possible, SSL certificates and strong encryption between client and server need to be used. 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 (Sanders, Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1), 2010).

In the case of portable devices, it is possible to prevent MITM attacks when the devices are never connected directly to Wi-Fi routers of insecure networks. In such connections, additional protection should be used whenever possible, for example, HTTPS Everywhere or ForceTLS.

DNS spoofing is mostly passive by its nature, so it is difficult to defend. In very targeted attacks it is quite possible that the victim will never know that he has been attacked. But there are a few things that can be done to defend (Sanders, 2010A):

- securing of internal machines.
- no reliance on DNS for secure systems.
- use of IDS, and
- use of DNSSEC.

Also, a few things can be done to defend against session hijacking (Sanders, 2010B):

- doing online banking from home,
- being cognizant and keeping an eye out for things that seem unusual, and
- securing own internal machines; such attacks are mostly executed from inside the network.

SSL hijacking is virtually undetectable from the server side, but some things can be done from the client's side (Sanders, 2010C):

- insurance of secure connections using HTTPS,
- doing online banking from home, and
- securing own internal machines.

To ensure reliable identification of devices, the participants in communication in the IoT, IoT must provide greater application of public-key cryptography (PKC). The main challenge with the use of PKC is validating whether the public key is authentic, and belongs to a certain person, or it was replaced by an attacker. Verification requires a digital certificate issued by a trusted certification authority (CA). Once the communication starts safely, the risks associated with the MITM attack are significantly reduced.

However, public key infrastructure (PKI) keys can still be compromised, and it can impact other devices. When an attacker gets access to the root key, he is in a position to sign malicious software and create fake certificates. The solution is to involve the "root of trust" (RoT) a set of functions in the trusted computing module that is always trusted by the computer's operating system (OS). (Jamie, 2016)

Finally, a recommendation to all users can be to avoid the functions "auto connect" and "Reply", and to avoid clicking on the embedded links from untrusted sources and the opening of not-asked attachments. It can be of help to ignore unexpected communications. also, a sudden change in business practice is a reason to check by using other means of communication whether a legitimate person tried to establish communication. Not jailbreaking phones and not using apps from untrusted sources are also recommended.

6 THE ECONOMIC ASPECT

It is very rare to find exact data on losses caused by MITM attacks. MITM attacks usually target individuals, and they do not publish their losses. Companies often don't want to tell customers that their products can be a victim of MITM attacks. Therefore, it is easy to conclude that the published attacks are the tip of the iceberg. Defining costs resulting from MITM attacks is even more difficult when MITM attacks are considered as a part of other major attacks, including DDoS.

On December 02, 2013, the Seattle Division of the FBI announced that it was aware of a fraud victimizing Washington state-based businesses, with "total loss experienced by the three area companies is roughly $1.65 million". (FBI Seattle, 2013)

Per SEC Consult and their analysis of the "firmware images of more than 4000 embedded devices of over 70 vendors, in which they paid their attention to cryptographic keys, they found more than 580 unique private keys distributed over all the analyzed devices. Correlating their data with data from Internet-wide scans (Scans.io and Censys.io) they found that their data set contained (SEC Consult, 2015):

- "The private keys for more than 9% of all HTTPS hosts on the web (~150 server certificates, used by 3.2 million hosts)
- the private keys for more than 6% of all SSH hosts on the web (~80 SSH host keys used by 0.9 million hosts)"

In addition, they recovered around 150 HTTPS

server certificates used by 3.2 million devices, together with 80 SSH host keys used by at least 0.9 million devices. In their analysis were included different devices: Internet gateways, modems, routers, IP cameras, VOIP phones, etc."

Such a situation in cryptography can result in large losses caused by future MITM attacks. The situation with recycling cryptographic keys becomes even more difficult when one considers that many of devices can be accessed from a public network. This allows MITM attack easy detection of credentials and/or session hijacking.

Earlier mentioned the Jeep hacking incident led to Fiat Chrysler recall of 1.4M vehicles, both cars and trucks. (AP, 2015) For the manufacturer, FCA US, the American arm of the Italian auto group, this meant a huge inconvenience, big losses in potentially sending of more than one million USB memories with patches for software, but these losses are bigger when a reputation loss and goodwill diminishing are included. On the other hand, for users, besides wasting time, it could also mean the loss of their (and not only their) lives.

Bearing in mind the possibility of attacks and their related losses, Internet users have a reason to think about sharing of risk with insurance companies. "Cyber insurance can provide a valuable and flexible tool for covering many types of cyber losses." (Watson, 2016) It is good to ensure coverage of the most probable attacks, in the broadest possible terms and conditions, in advance of a loss. But, to transfer risk successfully, with rapid developments in these evolving areas of coverage, the coverage needs to be flexible and to act upon at the time of loss through proactive claims advocacy.

7 CONCLUSION

IoT devices' protection depends on many factors, starting from the producer of the device and their conception of the device protection to the end user and their awareness of possible risks, and needs for device software patching whenever an update is released. Among all factors, the most conspicuous are device identification and the encryption of communication between the device and its user. Such communications demand certificates to identify each device. Because there are, and there will be billions of devices, it is to be expected that IoT devices will be insecure very frequently, at least during the period from the moment when a device was connected to the network, up to the moment when a vulnerability is discovered. The problem is even heavier when the factor "user" is included in the analysis. It is hard to expect that each user will keep their device software updated. Another problem can lay in the tendency to insist on constant cheapening of production and products. Cheaper products may mean less protection against attacks on the device. The consequences are numerous, and one of them is that an attack that was carried out at a network weak point can be transferred to other devices in the network.

The attackers are frequently at an advantage, both in terms of knowledge and in terms of technology at their disposal. MITM attacks because of their specificity and diversity remain effective technology for carrying out attacks and acquiring illegal benefits. Although they are performed in different versions, they are based on the same idea. An MITM attack is often combined with other attacks or built into them.

MITM attacks usually target individuals, and the attacks often remain undiscovered and unrecorded in the statistics. When economic operators are under attack, the attacks often remain hidden from the public to preserve the company's image. Only in large-scale attacks, it comes to light the extent of the damage caused. Despite difficulties in collecting relevant data, this analysis of examples clearly showed the possible extent of damage that can be caused by MITM attacks. Also, the analysis showed that the increasing number of IoT devices provides attackers with more targets.

The research has shown the great potential of IoT, but also the risks that may occur from insufficient protection, and that for IoT users, at least, a good idea is not to use public Wi-Fi in situations when doing anything sensitive and/or confidential. As mentioned, it is not possible to have a magic wand that will provide a whole protection, but there are two magic words: prevention and proactiveness!

Finally, the research showed that the null hypothesis H0 is rejected. The research showed that MITM attacks, although a rather old technology, are not rare and, even more, can cause damage to the attacked IoT. That way the alternative hypothesis H1 is proven.

WORKS CITED

Amato, F., & Kirschbaum, F. (2010). *evilgrade, 'You still have pending upgrades!'*. Retrieved from Defcon: https://www.defcon.org/images/defcon-18/dc-18-presentations/Amato-Kirschabum/DEFCON-18-Amato-Kirschabum-Evilgrade.pdf

AP. (2015, July 27). *Jeep Hacking Incident Leads to Fiat Chrysler Recall of 1.4M Vehicles*. Retrieved from Claims Journal: http://www.claimsjournal.com/news/national/2015/07/27/264766.htm

Barcena, M. B., & Wueest, C. (2015, Mar 12). *Insecurity in the Internet of Things.* Retrieved from Symantec: https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf

Cisco. (2016, Dec 16). *Different Things Need To Be Protected.* Retrieved from Cisco IBSG projections: https://www.cisco.com/c/dam/en_us/about/security/images/csc_child_pages/white_papers/iot-figure1.jpg

Cisco. (n.d.). *Threats in Borderless Networks.* Retrieved from LearnCisco: http://www.learncisco.net/courses/iins/common-security-threats/threats-in-borderless-networks.html

Covington, M. (2016, Oct 8). *Free Wi-Fi and the dangers of mobile Man-in-the-Middle attacks.* Retrieved from betanews: http://betanews.com/2016/10/08/free-wi-fi-mobile-man-in-the-middle-attacks/

DuPaul, N. (n.d.). *Man in the Middle (MITM) Attack.* Retrieved Nov 28, 2016, from Veracode: http://www.veracode.com/security/man-middle-attack

Edwards, R. (2016, Aug 119). *Simple Man-in-the-Middle Script: For Script Kiddies.* Retrieved from Wonderhowto: http://null-byte.wonderhowto.com/news/simple-man-middle-script-for-script-kiddies-0168192/

Evans, D. (2011, Apr). *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything.* Retrieved from Cisco - White Paper: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

FBI Seattle. (2013, Dec 02). *'Man-in-the-E-Mail' Fraud Could Victimize Area Businesses.* Retrieved from The Federal Bureau of Investigation - Seattle Division: https://archives.fbi.gov/archives/seattle/press-releases/2013/man-in-the-e-mail-fraud-could-victimize-area-businesses

Gallagher, S. (2016, Oct 21). *Double-dip Internet-of-Things botnet attack felt across the Internet.* Retrieved from arsTECHNICA: http://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/

Gregg, M. (2015, Dec). *How new technologies are reshaping MiTM attacks*. Retrieved from TechTarget: http://searchnetworking.techtarget.com/tip/How-new-technologies-are-reshaping-MiTM-attacks

Gregg, M. (2015, 12 11). *Six ways you could become a victim of man-in-the-middle (MiTM) attacks this holiday season.* Retrieved from The Huffington Post: http://www.huffingtonpost.com/michael-gregg/six-ways-you-could-become_b_8545674.html

How to conduct a simple man-in-the-middle attack. (2014). Retrieved from wonderhowto: http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/

Jamie. (2016, Feb 12). *Protecting IoT Against Man-in-the-Middle Attacks*. Retrieved from Bizety: https://www.bizety.com/2016/02/12/protecting-iot-against-man-in-the-middle-attacks/

Jasek, S. (2016). *Gattacking Bluetooth smart devices.* Retrieved from blackhat: https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf

Jasek, S. (2016, Jul-Aug). GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy. *Black Hat USA 2016* (p. 49). Mandalaya Bay, Las Vegas: Black hat. Retrieved from Black hat: https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool.pdf

Kapil, J., Manoj, J., & Borade, J. (2016). A Survey on Man in the Middle Attack. *IJSTE, 2*(9), 277-280. Retrieved from http://www.academia.edu/24382368/A_Survey_on_Man_in_the_Middle_Attack

Marlinspike, M. (2014, Feb 18). *sslstrip*. Retrieved from KaliTools: http://tools.kali.org/information-gathering/sslstrip

Marquess, K., & et al. (2010, Jun 30). *Bluetooth specification version 4.0.* Retrieved from Bluetooth.org: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737

McAfee. (2016). *McAfee Labs Threats Report, September 2016.* CA: Santa Clara: Intel Security.

Montoro, M. (2014). *Cain & Abel*. Retrieved from Oxid.it: http://www.oxid.it/cain.html

Ornaghi, A., & Valleri, M. (2015, Mar 14). *Ettercap project*. Retrieved from Ettercap: https://ettercap.github.io/ettercap/index.html

Sanders, C. (2010, Mar 17). *Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1).* Retrieved from windowsecurity: http://www.windowsecurity.com/articles-

tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

Sanders, C. (2010A, Apr 7). *Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing.* Retrieved from Windowsecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html

Sanders, C. (2010B, May 05). *Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking.* Retrieved from Windowsecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html

Sanders, C. (2010C, Jun 9). *Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking.* Retrieved from WindowSecurity: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html

SEC Consult. (2015, Nov 25). *House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide.* Retrieved from Blog.sec-consult: http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html

Simko, C. (2016, Feb 26). *Man-in-the-Middle Attacks in the IoT*. Retrieved from GlobalSign Blog: https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/

Song, D. (2001). *dsniff.* Retrieved from monkey.org: https://www.monkey.org/~dugsong/dsniff/

Spring, T. (2016, Aug 11). *Bluetooth Hack Leaves Many Smart Locks, IoT Devices Vulnerable*. Retrieved from threatpost: https://threatpost.com/bluetooth-hack-leaves-many-smart-locks-iot-devices-vulnerable/119825/

Watson, W. T. (2016, Oct 28). *The "Internet of Things" attacks.* Retrieved from Willis Towers Watson Wire: http://blog.willis.com/2016/10/the-internet-of-things-attacks/

Received for publication: 14.01.2017
Revision received: 13.02.2017
Accepted for publication: 01.04.2017

How to cite this article?

Style – **APA** *Sixth Edition:*

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017, July 15). Internet of things and the Man-In-The-Middle attacks – Security and economic risks. (Z. Čekerevac, Ed.) *MEST Journal, 5*(2), 15-25. doi:10.12709/mest.05.05.02.03

Style – **Chicago** *Sixteenth Edition:*

Cekerevac, Zoran, Zdenek Dvorak, Ludmila Prigoda, and Petar Cekerevac. "Internet of things and the Man-In-The-Middle attacks – Security and economic risks." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 5, no. 2 (July 2017): 15-25.

Style – **GOST** *Name Sort:*

Cekerevac Zoran [et al.] Internet of things and the Man-In-The-Middle attacks – Security and economic risks [Journal] // MEST Journal / ed. Čekerevac Zoran. - Toronto - Belgrade : MESTE, July 15, 2017. - 2 : Vol. 5. - pp. 15-25.

Style – **Harvard** *Anglia:*

Cekerevac, Z., Dvorak, Z., Prigoda, L. & Cekerevac, P., 2017. Internet of things and the Man-In-The-Middle attacks – Security and economic risks. *MEST Journal,* 15 July, 5(2), pp. 15-25.

Style – **ISO 690** *Numerical Reference:*

Internet of things and the Man-In-The-Middle attacks – Security and economic risks. **Cekerevac, Zoran, et al.** [ed.] Zoran Čekerevac. 2, Toronto - Belgrade : MESTE, July 15, 2017, MEST Journal, Vol. 5, pp. 15-25.