MEST Journal
DOI 10.12709/mest.13.13.01.04

SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE ATTACKS

Zoran Cekerevac
MESTE, Belgrade, Serbia
https://orcid.org/0000-0003-2972-2472

Petar Cekerevac
Independent researcher, Belgrade, Serbia
https://orcid.org/0000-0001-6100-5938

Lyudmila Prigoda
Maikop State Technological University, Maikop, Russia
https://orcid.org/0000-0002-4762-3892

Fawzi Al-Naima
Al-Kut University College, Wasit, Iraq, and Department of Computer Eng., Al-Nahrain University, Baghdad, Iraq
https://orcid.org/0000-0003-0930-5073

JEL Category: **G32, M15**

Abstract

This paper presents a detailed analysis of Man-in-the-Middle (MITM) attacks, covering their technology, historical examples, economic consequences, and managerial prevention activities. The study overviews modern Internet trends and discusses the weaknesses of current security measures, such as Secure Sockets Layer and Transport Layer Security protocols, and the complexity of two-way trust relationships. Various techniques for launching MITM attacks are considered, including Address Resolution Protocol cache poisoning, Domain Name Server spoofing, session hijacking, and Secure Sockets Layer hijacking. A chronological overview of some well-known MITM attacks highlights a shift from laptops to mobile devices. It emphasizes the vulnerability of Bluetooth low-energy devices, estimating around 80% of such devices are susceptible to MITM attacks. Overall, this paper provides a perceptive analysis of MITM attacks, their past and current manifestations, and the significant economic impact they can have on computer systems and users and underscores the crucial need for robust security measures.

Keywords: *Babington Plot, computer applications, computer networks, Internet, MITM.*

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

1 INTRODUCTION

In 2011, Cisco predicted that by 2020, there would be 50 billion devices connected to the Internet. The widespread deployment of the Internet of Things (IoT) was expected to lead to a significant transformation in our comprehension and the evolution of the Internet (Evans, 2011). It seems that expectations were too optimistic. In the meantime, unexpected events took place and greatly influenced the development of the Internet, devices, and applications. As reported by Statista, about 15.14 billion IoT devices were used worldwide in 2023 (Vailshery, 2023). We can add approximately seven billion mobile phones and two billion personal computers. It is easy to conclude that the Internet was connecting over 24 billion devices in 2023.

New software applications emerged alongside the widespread use of new devices. They enhanced the quality of life, but also brought about a significant increase in risks.

It is fine when everything is connected to the Internet and can exchange data according to user wishes. But, on its way to its final destinations, data passes through all TCP/IP model layers where many risks lurk. One can add a new potential risk layer, the extensive use of Cloud storage. The possibility of an attack on this layer is high, starting with brute force attacks at password-based attacks and including possible data change at the Session layer using man-in-the-middle (MITM)[1] attacks.

This paper presents famous MITM attack cases and their economic consequences. For those unfamiliar with MITM attack technology, in Section 3, we explained an example of a communication scheme shown in Fig. 1. We also recommended other literature sources with more in-depth details to enhance comprehension of MITM attacks.

2 METHODS AND HYPOTHESES

The methodology applied in this research includes the systemic-functional approach to the phenomena analysis. In justification of theoretical propositions and findings, the authors used the hypothetico-deductive method, axiomatic method, analytical-deductive method, comparative method, scientific induction and deduction, synthesis, and comparative analysis.

At the turn of the century, research efforts were directed towards MITM attacks. With the advancements in computer protection technology, the authors of this paper proposed a research question:

Are MITM attacks still a threat?

They entered the research with the following hypothesis:

H_o – The MITM attack is an old and outdated technology that cannot harm modern computer systems and their users, so it is no longer in use.

The authors also set the alternative hypothesis:

H_a – MITM attacks still exist and can harm modern computer systems and their users.

3 MITM TECHNOLOGY

An MITM attack can be visualized as a game of the broken telephone when words are passed from the first participant to a row of participants up to the final participant. The message often reaches the last person in the row modified, consciously or unconsciously. In an MITM attack, an intermediate participant manipulates the messages of two legitimate participants.

Man-in-the-middle attacks have been happening since ancient times. Only the means were different. One of the most famous MITM attacks was the Babington Plot. It took place in 1568. Communications between Mary Stuart and her supporters regarding the plot to assassinate Queen Elizabeth I were intercepted by a third party (Sir Francis Walsingham). Altering the contents of the messages revealed the identities of those involved in the plot and resulted in their execution (Ecuron, 2023).

Most modern Internet applications use encrypted connections provided by SSL/TLS protocols to provide services securely. SSL/TLS can create a two-way trust relationship, but it is rather complex for administration. Often, only one party

[1] Also known as Manipulator-in-the-Middle or Machine-in-the-Middle

authenticates the connection. That represents a weakness that an attacker can exploit.

A modern MITM attack employs various techniques to intercept communication between two nodes. The attacker can usurp the proxy role by disconnecting their victims' communication.

The MITM attack example in Fig. 1 was thoroughly analyzed in the paper by Cekerevac, Dvorak, Prigoda, & Cekerevac (2017). The attacker's idea is to replace the public keys of Victim A (bank client) and Victim B (bank) in victims' communication with his public key. The attacker's main challenge is how to get involved in communication. Once successfully positioned, he can manipulate communications or use eavesdropping.

How it might look in the case of an attack on Office 365 is shown in Fig. 2. In credential phishing, the MITM server acts as a proxy. It presents the destination's login page to the victim and passes on any received username and password to the destination URL. In the case of multi-factor authentication (MFA), it presents the MFA request to the user for further input and forwards any responses to the destination. Because the MITM server is between secure connections, it can decrypt data from the user and extract the username and password. It then re-encrypts the traffic and sends it to the destination website. When authentication is completed, the final step is for the destination website to send a session cookie to the user. Session cookies are valuable as they manage all the information that needs to be stored during the victim's interaction with the website. An attacker can decrypt and extract the session cookie before sending it to the user (Arndt, 2023).

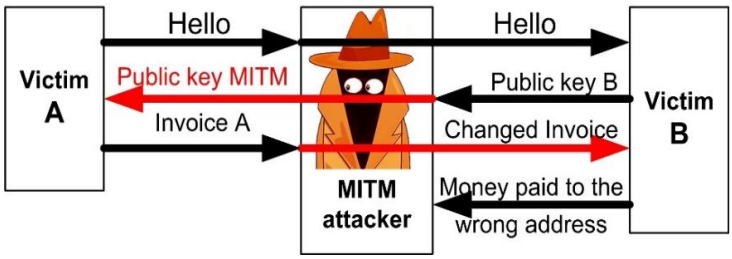

Fig. 1 An example of the MITM attack (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017)

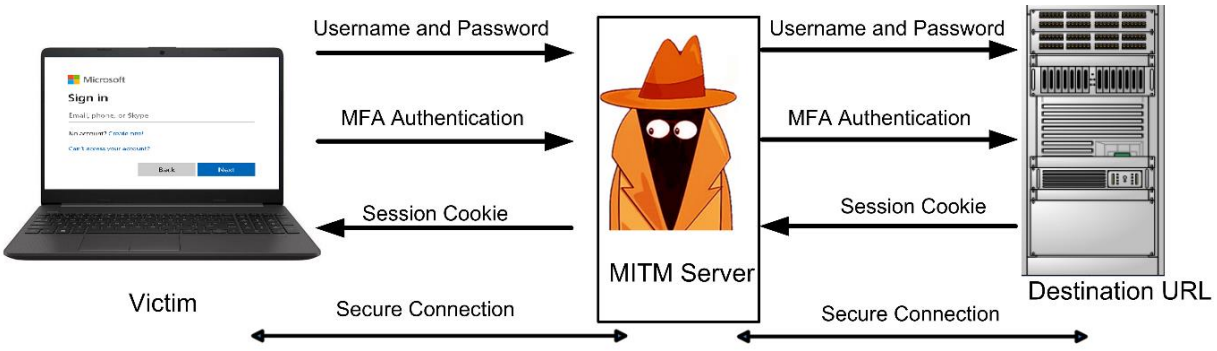

Fig. 2 The MITM server intercepts all steps of authentication. (Source: Authors, based on (Arndt, 2023))

The MITM attacks can start with (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017):

- Address Resolution Protocol (ARP) cache poisoning. The attacker manipulates ARP tables to intercept and redirect network traffic between two parties.
- DNS spoofing. The attacker forges DNS responses to redirect users to malicious websites or intercept sensitive information.
- Session hijacking, including side-jacking, evil twin, and sniffing. The attacker steals or impersonates a user's session token to gain unauthorized access or perform actions on their behalf.

- SSL Hijacking. The attacker intercepts and decrypts SSL/TLS encrypted communications by presenting fake certificates.

Here are some other common examples of Man-in-the-Middle (MITM) attacks, such as:

- Wi-Fi pineapple attacks - The attacker exploits Wi-Fi vulnerabilities to intercept and manipulate network traffic.
- IP spoofing - The attacker manipulates the source IP address to impersonate another person or device on the network.
- Evil Twin attacks - The attacker creates a fraudulent wireless access point (AP) to trick users into connecting and intercepting their traffic.
- Email interception - The attacker intercepts and reads email messages exchanged between two email servers.
- SSL stripping - The attacker downgrades an encrypted connection to an unencrypted one, allowing them to intercept sensitive information.
- Bluetooth hijacking - The attacker intercepts and manipulates Bluetooth communication between devices.

In the past, MITM attacks predominantly targeted laptops, but now mobile phones are becoming the main target of attacks. The risk is increasing because many users do not even think about their data protection. Significant risks also arise from the Internet of Things (IoT) inclusion in networks. Each of the connected devices is a possible point of intrusion into the network.

MITM attacks can be performed in many ways using a variety of tools. Some of such tools are:

- Ettercap – a comprehensive suite for MITM attacks that includes many features for network and host analysis and supports the dissection of many protocols (Ornaghi & Valleri, 2015).
- evilgrade – a modular framework that allows injecting fake updates and making hostname redirections (Amato & Kirschbaum, 2010).
- Dsniff – “a collection of tools for network auditing and penetration testing. Sshmitm and webmitm implement active MITM attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI” (Song, 2001).

There is also a risk in Bluetooth communication. Some say that the Bluetooth operating range is small and an MITM attacker must be close to both attacked devices. That is true, but Bluetooth Low Energy (BLE) devices can have a working range of more than 100m. Furthermore, in some cases, the devices do not even need to be close to each other. The attacker can relay packets remotely via the Internet (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017).

Many Bluetooth devices used for keyless entry and mobile point-of-sales systems are vulnerable to MITM attacks. The BLE specification provides secure connections through link-layer encryption, device whitelisting, and bonding. But "companies too often do not implement correctly that protection and this lack could allow attackers to clone BLE devices” (Jasek, 2016). “Jasek estimates that 80% of BLE smart devices are vulnerable to MITM attacks” (Spring, 2016). Per this research, 80% of reviewed devices were incorrectly configured. That allows hackers to use tools like GATTacker to perform an MITM attack.

It is interesting to see how MITM attacks have adapted to today's circumstances. Here are some experiences (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017):

- Man-in-the-cloud (MITC). Cloud computing has become a standard for many users. Storage capacities are large enough and do not demand users to log on for each data transmission session. After the first authentication, they use a session token saved on the user's local computer. If an attacker steals the token, he can fully control the account.
- Man-in-the-browser (MITB). Many people use e-banking. In the MITB attacks, an attacker in some way inserts a Trojan into the victim's computer. When the victim attempts to visit the targeted URL, the malware injects specific HTML code into the original web page code to trick the user. If the user is not careful, he will not notice minor differences between the current and original user interface. After that, "banking services" will be "provided" by the attacker.

- Man-in-the-mobile (MITMO). Many users prefer to make their financial transactions over their smartphones. The MITMO attack focuses 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 is a real and significant challenge for out-of-band authentication systems (Gregg, 2015A).
- Man-in-the-app (MITA). Mobile apps can be vulnerable. MITA implies that an application does not perform certificate validation properly. An attacker inserts a self-signed certificate and exploits how the applications handle trust. He can communicate with the app directly. Then, the hacker can intercept application data, steal information, or impersonate the victim on the application (Gregg, 2015).
- MITM attacks on IoT. With the increasing development of IoT, MITM attacks have become a much bigger challenge. For example, close-to-home devices could be IoT refrigerators that display a user's Google calendar. Research showed that they did not validate SSL certificates. This slip could result in the mounting of an MITM attack and the user's Google credentials stolen (Gregg, 2015A).

After a successful MITM attack, an attacker can use it for identity theft, surveillance, financial exploitation, malware infection, business sabotage, and/or network exploitation (Martens, 2023).

4 RESEARCH RESULTS

Advances in encryption technology and network security have made MITM attacks more difficult to carry out. However, many successful MITM attacks resulted in identity theft, malware infiltration, and financial losses. Cofense Intelligence has identified trends in MITM attacks based on several tell-tale signs (Arndt, 2023):

- MITM attacks increased by 35% in volume, reaching inboxes between Q1 2022 and Q1 2023.

It has been found that the majority of MITM credential phishing attacks, specifically 94%, were aimed at O365 authentication.

At least one URL redirection was used in 89% of campaigns, while 55% used two or more.

After conducting extensive research, we have identified several major MITM attacks that occurred in the last decade.

4.1 DNSChanger botnet: 2007 – 2018

The DNSChanger botnet was a notorious cybercriminal operation active from 2007 to 2011. Initially, the botnet infected millions of computers globally, primarily targeting Windows-based systems. It spreads through various means, such as malicious email attachments, drive-by downloads, and software vulnerabilities. The cybercriminals behind the operation used the botnet for nefarious purposes, including distributing malware, injecting malicious advertisements, and conducting fraudulent activities.

In late 2009, NASA OIG and the FBI opened a joint criminal investigation against Rove Digital, a company suspected of being the source of DNSChanger botnet fraud. This botnet allowed the attackers to redirect millions of victims to websites of the attacker's choice, instead of the websites that victims intended to visit. The malware forced more than one hundred NASA computers to use Rove Digital's DNS servers instead of NASA's DNS servers, which placed them into a sort of botnet under the control of Rove Digital. The NASA OIG checked security records and determined that Session hijacking caused them losses that exceeded $65,000. Millions of computers were believed to be infected worldwide. Seven persons were charged with computer intrusions, wire fraud, and money laundering. Millions of dollars in accounts in Estonia, the United States, Cyprus, Denmark, and Austria have been frozen. In Estonia, real estate and other assets belonging to the defendants were seized (Zadig, 2012-2013).

DNSChanger botnet targeted the Domain Name System (DNS) responsible for translating human-readable domain names into IP addresses. It aimed to redirect users to malicious servers, allowing the attackers to control and manipulate internet traffic for their gain.

The DNSChanger botnet attacked numerous devices worldwide, including computers, routers, and other networked devices. It achieved this by

exploiting security vulnerabilities and spreading malware through infected websites or malicious email attachments.

Activated botnet changed the DNS settings within compromised devices, pointing them to rogue DNS servers controlled by the attackers. Victims' requests were redirected to malicious servers under the attackers' control instead of legitimate websites or online services. This setup allowed the attackers to intercept and monitor internet traffic, potentially leading to various malicious activities like phishing, data theft, and spreading further malware.

The impact of the DNSChanger MITM attack was extensive, affecting both individuals and organizations. Organizations faced risks from compromised internal traffic, compromised data integrity, and the potential for sensitive information leakage.

To combat the threat, cybersecurity organizations and law enforcement agencies worked together to dismantle the botnet infrastructure. With court approval, they arrested and prosecuted the individuals responsible for operating the DNSChanger botnet. Law enforcement also helped victims remove the malicious DNS settings from their devices and restore normal functionality. The security experts advised users on protection against similar MITM attacks and reducing the spread of malware across networks.

In 2011, with the help of a multinational collaboration between law enforcement agencies and cybersecurity organizations, the botnet was suppressed. However, some infected devices remained active because their users did not take any action to clean their systems.

In 2016, Proofpoint experts discovered several improvements in the implementation of the DNSChanger attack, including (Proofpoint, 2016):

- External DNS resolution for internal addresses.
- Steganography for concealment.
- Adding dozens of recent router exploits. At the end of 2016, there were 166 fingerprints, some working for several router models (in 2015 there were 55 fingerprints). Some were a few weeks old (13/09/2016) when the attack started around 28 October.
- When possible (in 36 cases) the exploit kit modifies network rules so the administrative ports are accessible from external addresses. It exposed the router to additional attacks like the Mirai botnet (Vailshery, 2023).
- The adware chain also accepted Android devices.

As of December 16th, 2016, DNSChanger EK appeared to be offline, and the malicious campaign stopped. However, any previously compromised routers (at least 56,000) were potentially still under the attacker's control. The campaign was widespread internationally, mostly in the USA (14%), Indonesia (12.9%), and Brazil (7.4%). Non-mobile computers were mostly attacked (68.4%). Mobiles followed (30.3%). Attacked visitors mostly used the Chrome browser (73.9%). From mobiles, visitors mostly used Android phones (66.5%) and tablets (11.5%). 12% of visitors used iPhones, and 9.8% used iPads (Proofpoint, 2016).

In 2017, law enforcement agencies and cybersecurity experts discovered that remnants of the botnet were still infecting computers worldwide. To combat this ongoing threat, cybersecurity experts launched a campaign to raise awareness and assist affected users in removing the botnet from their devices. The campaign provided resources for individuals to identify if their system was infected and offered guidance on how to mitigate the botnet's impact.

In 2018 a massive new DNS changing issue appeared. Chinese cybersecurity uncovered an ongoing malware campaign that hijacked over 100,000 home routers and modified their DNS settings to steal users' login credentials by redirecting them to malicious web pages, especially when they visited banking sites.

The campaign dubbed GhostDNS has many similarities with the infamous DNSChanger malware. According to the cybersecurity firm Qihoo 360's NetLab, just like the regular DNSChanger campaign, GhostDNS scans for the IP addresses of routers that use weak or no passwords. Then, it accesses the router's settings and changes the router's default DNS address to the one controlled by the attackers (Rocha, 2018).

The DNSChanger botnet attack served as a reminder of the critical role of DNS in Internet

communication and the risks associated with compromised DNS settings. To avoid such attacks users are advised to always use the latest firmware version and a strong password for their router.

4.2 MITM attack on Yahoo: 2011 – 2016

The largest-known breach of any company's computer network happened with Yahoo! in 2013. (Senouci, 2023) Digital thieves have taken over all 3 billion Yahoo user accounts data by that attack. In 2014, the company also disclosed a separate attack that affected 500 million accounts. Attackers came into a position to take data including names, birth dates, phone numbers, passwords, security questions, and backup email addresses. The data was encrypted with easy-to-crack security (Perlroth, 2017).

In 2016, Yahoo faced a significant security breach caused by the MITM attack. Yahoo admitted that one billion accounts were compromised (Khandelwal, 2016) (Henriques, 2016). The attackers employed various methods to carry out the MITM attack on Yahoo. It is believed that they exploited a combination of social engineering tactics, vulnerabilities within Yahoo's systems, and sophisticated techniques. By infiltrating Yahoo's network, the attackers were able to gain access to highly sensitive user information, including names, email addresses, telephone numbers, dates of birth, and passwords of millions of Yahoo users.

Furthermore, the attackers targeted Yahoo's "Account Management" tool, which enabled them to forge "cookies".[2] These forged cookies allowed the attackers to impersonate Yahoo users without needing their passwords and gain access to their accounts, potentially exposing further personal information.

The consequences of the Yahoo MITM attack were substantial. Apart from the immediate breach of personal data, the incident compromised user trust and had far-reaching implications. Customers' private information became vulnerable to misuse, such as identity theft, phishing attacks, and other fraudulent activities. The breach also impacted Yahoo's reputation, leading to public scrutiny and negative publicity.

Yahoo responded to the attack by launching an investigation, notifying affected users, and advising them to change their passwords. They also invalidated the forged cookies, patched security vulnerabilities, and enhanced their security measures to prevent future breaches. The incident prompted Yahoo to collaborate with law enforcement agencies and cybersecurity experts to identify the attackers and hold them accountable.

Court proceedings have also been initiated against Yahoo and Aabaco Small Business, LLC, which resulted in a proposed class-action settlement regarding data hacking incidents that occurred from 2013 to 2016, as well as in connection with data breaches that occurred at least from January to April 2012, although it does not appear that hackers took the data in that case. The settlement applies to those who had a Yahoo account at any time from January 1, 2012, to December 31, 2016 and resided in the USA or Israel. Under the Settlement terms, Yahoo has enhanced, or, through its successor, Oath Holdings Inc., continues to improve its business practices to improve the security of its users' personal information stored in its databases. Yahoo and Aabaco Small Business are obligated to pay $117,500,000 into the Settlement Fund, which is regulated to provide a minimum of two years of credit monitoring services to protect Settlement Class Members from future damages, or a cash alternative for those already have credit monitoring or identity protection. The settlement fund is obligated to provide monetary payments to individuals who incurred expenses, including loss of time, as well as to Yahoo users who paid for ad-free or premium Yahoo Mail services, and to users of Aabaco Small Business services, including business email. The settlement fund will also cover any costs related to the court process. In return, plaintiffs will drop their claims related to the Incidents (Case No. 5:16-MD-02752-LHK, 2020).

In conclusion, the 2016 MITM attack on Yahoo highlighted the critical importance of robust cybersecurity measures and the potential

[2] Small files that authenticate users and keep them logged in to their accounts.

consequences of large-scale data breaches. It served as a wake-up call for Internet users and organizations to prioritize personal information protection and strengthen their defenses against evolving cyber threats.

Verizon bought Yahoo for $4.48 billion in June 2017, but the price was reduced by $350 million from the original deal because of the breaches. Also, Verizon and Yahoo agreed to share certain legal and regulatory liabilities because of data breaches incurred by Yahoo (Tran, 2017).

The Verizon 2023 Data Breach Investigations Report (Hylender, Langlois, Pinto, & Widup, 2023) showed that:

- 74% of all breaches include the human element (via error, privilege misuse, stolen credentials, or social engineering).
- 83% of breaches involved external actors. The primary attackers' motivation is overwhelmingly financially driven at 95% of breaches.
- The primary methods that attackers use are stolen credentials, phishing, and exploitation of vulnerabilities.

Social Engineering attacks are very effective and highly lucrative for cybercriminals. Business Email Compromise (BEC) attacks have almost doubled across incident datasets.

4.3 Superfish: 2014

Superfish was a high-profile security incident and involved some Lenovo laptops sold between 2014 and 2015 (CISA, 2016). This incident was caused by the pre-installed adware program called Superfish, which had severe implications for user privacy and security. Superfish was designed to inject targeted advertisements into users' web browsers by analyzing images on websites. To achieve this, Superfish utilized an MITM attack.

Superfish installed a self-signed root certificate on affected laptops to inject the ads. This certificate allowed Superfish to intercept and decrypt secure HTTPS connections between the user's browser and websites. Superfish undermined https security by acting as a proxy and decrypting the traffic without the user's knowledge or consent (Goodin, 2015).

By conducting an MITM attack, Superfish could inject its ads into websites, even if they were not designed to show ads. This invasive behavior compromised users' browsing experience, flooded their screens with unwanted advertisements, and potentially exposed them to malicious content.

The use of a self-signed root certificate presented significant security risks. Normally, trusted certificate authorities issue SSL/TLS certificates to ensure the authenticity of encrypted communications. Superfish's self-signed certificate bypassed this crucial step. Attackers can exploit vulnerabilities to perform malicious acts. This exposes users to potential attacks by cybercriminals who exploit security gaps. Utilizing the same certificate, attackers could impersonate legitimate websites, intercept sensitive data such as login credentials or financial information, and launch other nefarious activities.

Once the Superfish controversy came to light, it sparked widespread concern among users, security experts, and the technology community. Lenovo faced significant backlash for pre-installing such intrusive adware on their devices. They apologized and promptly released a removal tool to uninstall Superfish and remove the root certificate from affected laptops.

The aftermath of the Superfish incident showed manufacturers and users the potential threats posed by pre-installed software and the need for transparency and security checks within the supply chain.

4.4 Cloudflare Heartbleed: 2017

The public became aware of the Heartbleed bug in 2014. It was a major security flaw in the OpenSSL encryption software those days. That vulnerability was easy to exploit. In addition, it was difficult to detect if an attacker used it.

OpenSSL is one of the best-known SSL implementations. It enables systems to communicate using SSL encryption. The initial release was in 1998, and OpenSSL worked correctly until 2011 when Robin Seggelmann added the faulty Heartbeat feature in an experimental software version. That version passed reviews and went into use. Neither reviewers nor users noticed it. It has been discovered that an OpenSSL vulnerability was present and active between March 2012 and April 2014. Those using older versions (before 1.0.1) were not at risk (Kiprin, 2021).

Heartbleed was a flaw within the implementation of the OpenSSL's Transport Layer Security (TLS) heartbeat feature. This feature allowed secure communication between servers and clients by periodically sending small packets of data to verify that the connection was still active. However, due to a coding error in OpenSSL, an attacker could send a specially crafted malicious heartbeat request, causing the server to leak random chunks of its memory.

The exploit enabled the attacker to retrieve sensitive information from the server's memory, which could include usernames, passwords, private digital keys, and even decrypted data. This kind of attack facilitated potential unauthorized access to confidential information and enabled cybercriminals to present themselves as trusted servers.

In 2017, the Cloudflare Heartbleed incident showcased a potential vulnerability in the widely used OpenSSL cryptographic software library. This vulnerability allowed attackers to carry out an MITM attack, potentially exposing sensitive data transferred between servers and clients.

The Cloudflare Heartbleed incident specifically refers to the impact that this vulnerability had on Cloudflare's content delivery network (CDN). As one of the largest CDN providers, Cloudflare's infrastructure was widely used by numerous websites, making the potential scale of the attack significant.

Upon the discovery of the vulnerability, Cloudflare immediately acted to remediate the issue by patching the affected systems and deploying the necessary security measures. They informed their customers, advised them to update their SSL certificates and private keys, and recommended that users change their passwords as a precautionary measure. Cloudflare has revoked and reissued over 100,000 certificates (Sullivan, 2021).

While the full extent of the exposure and any potential unauthorized access remains unclear, the impact of the Cloudflare Heartbleed incident raised awareness regarding the importance of promptly patching software vulnerabilities and conducting thorough security audits.

Although the Cloudflare Heartbleed attack itself is not an MITM attack, it is significant because in the attack exploited vulnerability can be used in MITM attacks to compromise the security of client-server communications. The Heartbleed incident served as a reminder that even widely trusted and well-established security protocols can contain flaws that cybercriminals can exploit. Unfortunately, it turns out that it is still common for systems to be vulnerable to Heartbleed (Venter, 2023).

4.5 KRACK Attack: 2017

The KRACK attack (Key Reinstallation Attack), discovered in 2018, targeted the WPA2 (Wi-Fi Protected Access II) protocol, which is widely used for securing Wi-Fi networks. It exploited vulnerabilities in the four-way handshake process of the WPA2 protocol and an attacker can use it in an MITM attack.

The KRACK attack leverages the fact that a four-way handshake, used to establish a secure connection between a client and an access point, can be manipulated. By forcing the reuse of a one-time encryption key during the handshake, an attacker can trick the client device into reinstalling a previously used key. This key reinstallation vulnerability allows the attacker to decrypt and/or forge data packets transmitted over the Wi-Fi network (Vanhoef & Piessens, Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse, 2017). Attackers can intercept and view sensitive information transmitted over Wi-Fi, such as passwords and credit card details. Additionally, the attacker could inject malicious content into the data stream, potentially leading to further compromise or exploitation.

The KRACK attack had a significant impact on a vast number of devices and Wi-Fi networks worldwide. Both client devices (such as smartphones, laptops, and IoT devices) and Wi-Fi access points were vulnerable to the attack. The attack vector did not rely on any specific software or implementation flaw but rather exploited weaknesses in the WPA2 protocol itself.

Once the KRACK vulnerability was discovered, major technology companies and vendors, including device manufacturers and network equipment providers, released patches and updates to address the issue. They advised users to apply these updates promptly to stay protected.

The KRACK attack highlighted the importance of using updated software and firmware, regular

security patching, and following best practices for securing Wi-Fi networks. It also reinforced the need for end-to-end encryption and the use of additional security measures like VPNs (Virtual Private Networks) to protect data transmitted over Wi-Fi networks, mitigating the risk of MITM attacks.

Currently, the most convenient, although not complete, solution for authentication, and prevention of KRACK and offline dictionary attacks is the WPA3 wireless security standard, which is not supported by all devices. Unfortunately, even WPA3 is not immune to all threats. Vanhoef and Ronen (2019) published several security flaws in WPA3 in 2019. This is about a set of security protocol vulnerabilities collectively known as Dragonblood (Irei & Scarpati, 2022). It refers to physical and temporal attacks that allow an attacker to force devices to revert to WPA2 or enable offline dictionary attacks.

4.6 Efail Attack: 2018

The Efail attack, discovered in 2018, targeted encrypted email communications and exploited vulnerabilities in the way certain email clients handle the OpenPGP and S/MIME encryption standards. It was an MITM attack that took advantage of how email clients handle encrypted content. It relied on manipulating the HTML rendering of encrypted emails to extract the plaintext content from the encrypted sections. By altering specific parts of the encrypted email, the attacker could trick the email client into sending the decrypted content or its metadata back to the attacker's server (EFAIL, 2018).

The vulnerability is directed against the content of the email and not against the recipient, The attack exploited both the design limitations and implementation flaws in certain email clients, particularly those that automatically decrypted or parsed encrypted email content for the convenience of the user. This allowed adversaries to bypass the inherent security provided by OpenPGP and S/MIME encryption standards. The Efail attack has been thoroughly analyzed by Poddebniak and colleagues in their research paper (2018).

The impact of the Efail attack was significant since it affected various email clients. However, it is important to note that the attack did not directly target the encryption algorithms themselves but rather the email client's handling of the encrypted content.

Once the Efail vulnerability was disclosed, the first recommendation was to disable PGP/GPG or S/MIME in email clients (Ashford, 2018). Researchers collaborated with affected email client vendors to address the issue and release necessary patches. In response, many email clients added necessary security improvements to prevent further vulnerability exploitation.

To protect against Efail and similar MITM attacks, users must keep their email clients up to date. Additionally, adopting secure communication protocols like TLS and using end-to-end encrypted messaging platforms can add an extra layer of protection to email communications.

The Efail attack highlighted the importance of continuous security assessments and improvements in encryption standards and the need for users and organizations to stay vigilant and proactive in safeguarding their confidential email communications.

4.7 Exodus: 2019

In 2019, security officers of Lookout discovered a significant cyber-attack, on iOS and Android, the "Exodus" attack that can be used in MITM attacks. It involved sophisticated techniques for intercepting and manipulating encrypted communications between users and servers (Vijayan, 2019).

The attack got its name after the malicious mobile malware utilized to carry out the attack. It involved the installation of malicious software on the compromised devices, which allowed the attackers to gain control over the encrypted connections. Once installed, the malware could intercept and redirect encrypted traffic, decrypt it, and then re-encrypt it before forwarding it to its intended destination. The attackers got a chance to intercept and manipulate the encrypted data by compromising the security and privacy of the victims. The Android version had full root access to the device, whereas the iOS version could only extract a limited set of data accessible via iOS APIs. Exodus for Android could keep running even when the screen is switched off.

The attackers achieved that by exploiting vulnerabilities in the targeted systems or leveraging social engineering techniques to trick users into downloading and installing a seemingly legitimate application previously bundled with malicious software. Google removed those apps after the company was notified of the problem. Security Without Borders estimated that there were potentially one thousand or more infections. Lookout said that their telemetry showed the attacks focused purely on Italian IP addresses, and the risk for other users was negligible (Vijayan, 2019).

Exodus was particularly concerning because it targeted encrypted communications commonly considered secure. By compromising trust, the attackers undermined the effectiveness of encryption protocols and put sensitive data at risk.

To protect against Exodus, it is crucial to adhere to security best practices such as keeping software and devices up to date, being cautious when downloading applications or clicking on suspicious links, using strong encryption protocols, and regularly monitoring network traffic for any signs of malicious activity.

4.8 Adversary-in-the-Middle: 2023

Recently, cybersecurity experts at Microsoft Defender detected a sophisticated attack that targeted banks and financial services organizations. This attack involved two stages - an adversary-in-the-middle[3] (AITM) phishing attack and a subsequent business email compromise (BEC) activity. What is concerning about this incident is that it exploited trusted relationships and came from a compromised vendor (Microsoft, 2023).

The attackers used an indirect proxy, which is different from the usual reverse proxy techniques. That allowed them to have control over phishing pages and steal session cookies. They also employed session replay attacks and took advantage of weak multifactor authentication (MFA) policies to modify MFA methods without being challenged. Furthermore, they conducted a second-stage phishing campaign that targeted the contacts of the initial victim, sending out over 16,000 emails.

Dealing with this attack requires more than standard measures to address identity compromise. Organizations affected by this attack need to revoke session cookies, undo any MFA modifications made by the attackers, and actively hunt for similar threats. The attackers, in this case, were associated with the Storm-1167 threat actor, according to Microsoft's classifications (Microsoft, 2023).

Adversary-in-the-middle attacks aim at intercepting and compromising user authentication processes for malicious purposes. In this attack, the adversaries positioned themselves between users and the targeted service, obtaining credentials and intercepting MFA to obtain session cookies. With these stolen session cookies, they gained access to user resources, carried out business email compromises, and engaged in other malicious activities.

Unlike previous campaigns, this attack did not rely on the reverse proxy method commonly used by AITM kits. Instead, it used an indirect proxy approach, which involved the target application's login page on a cloud service impersonating. By controlling the phishing website, the attackers could modify content and avoid detection. There were no proxy HTTP packets used between the victim and the website during the AITM attack unlike traditional attacks (Microsoft, 2023).

When the victim entered their login information, a fake multi-factor authentication page was displayed. The attackers obtained the MFA token from the user and used it to access the session token, starting a session with the authentication provider. Then, the victim was redirected to another page.

This attack underscores the complexity of AITM attacks and emphasizes the need for comprehensive security defenses. Organizations must remain vigilant and implement robust security measures to mitigate the risks posed by these evolving threat techniques. Storm-1167

[3] An adversary-in-the-middle (AitM) attack is also known as a man-in-the-middle (MITM) attack. (Hypr, 2023) (Rowe, 2023)

attack technology is discussed in detail in the Microsoft Security Blog (Microsoft, 2023).

4.9 BLUFFS attack

Researchers from Eurecom have recently discussed a new set of attacks called 'BLUFFS' that have the potential to compromise the secrecy of Bluetooth sessions, paving the way for MITM attacks. These attacks target two newly found architectural flaws within the Bluetooth standard that specifically impact the derivation of session keys used for decrypting data during communication. These vulnerabilities are not limited to any hardware or software configuration, as they stem from fundamental design weaknesses in Bluetooth. Due to the widespread usage of Bluetooth as a wireless communication standard, BLUFFS attacks can affect laptops, smartphones, and other mobile devices (Toulas, 2023).

The primary objective of BLUFFS is to undermine the forward and future secrecy of Bluetooth sessions, thereby compromising the confidentiality of data exchanged between devices. That is accomplished through capitalizing on flaws in the session key derivation process. Through these vulnerabilities, an attacker can launch a brute-force attack and force the derivation of a short, weak, and predictable session key (SKC) to decrypt past communications and manipulate future ones. The attack takes place in several phases, see Fig. 3.

To successfully execute a BLUFFS attack, the perpetrator must be within Bluetooth range of the targeted victims and pose as one of the devices involved in the session. By impersonating one device, an attacker can negotiate with the other device to establish a weak session key by proposing the lowest possible key entropy value while using a constant session key diversifier.

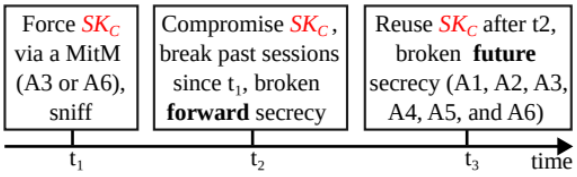

Fig. 3 Attack steps (Antonioli, 2023)

The BLUFFS attack can be of six different types, encompassing various combinations of impersonation and MITM techniques. These attacks are effective regardless of whether the targeted devices support Secure Connections (SC) or Legacy Secure Connections (LSC). BLUFFS impacts all versions of Bluetooth up to and including Bluetooth 5.4, released in February 2023, and Bluetooth 4.2, released in December 2014. The research conducted by Eurecom involved the efficacy of BLUFFS testing on different devices. All of them were susceptible to at least three of six BLUFFS attacks.

Bluetooth SIG, the organization responsible for licensing Bluetooth technology, advised implementing measures to mitigate the risks posed by the BLUFFS attacks. These measures include rejecting connections with low key strengths below seven octets, utilizing 'Security Mode 4 Level 4' to ensure strong encryption, and operating in “Secure Connections Only” mode while pairing (Toulas, 2023).

4.10 Mobile-in-the-middle

In sensitive information searches, fraudsters often use the proven MITM method of attack (Stockley, 2021). Due to the prevalence of mobile devices, MITM attacks often use so-called "evil twins" wireless networks. Compromised networks use the same name as legitimate ones. Therefore, they can easily trick victims and their devices that they belong to legitimate users.

MITM attacks are hard to detect because they are not in the victim's mobile device. During communication, the victim's mobile device and legitimate systems think they are communicating directly although the communication is over the attacker. One of the most significant MITM risks for smartphone users is communication over public wireless networks. Traced's research found that 5% of public networks were subject to an active MITM attack (Stockley, 2021). The attack can be by directly compromising a legitimate router, which allows the attacker to control the victim's connections to everything on the network. Router vulnerabilities allowed criminals to own hundreds of thousands of routers. MITM attacks that alter DNS traffic and lead victims to fake sites are just one of the possible burdens when attackers own the victim's gateway.

Not only Wi-Fi networks but also 5G networks are vulnerable to MITM attacks. At Black Hat 2019, security professionals demonstrated that it is possible to communicate with devices using a fake

base station. In doing so, it is possible to collect critical information about the device, including the type, operating system, version, and IMSI number[4]. Some MITM attacks do not require the presence of the mobile device owner. They can record the messages the device sends and play them back later. That was the case with Apple when it introduced the ability to buy transport tickets without unlocking the phone. Researchers at the University of Birmingham have found a way to reproduce a payment message, changing it so it can be sent to any wireless payment reader. That would allow an attacker to pay anything, in any amount, and at any time.

Working from home has become a permanent reality, so protecting against MITM attacks has become an obligation, not an option. If the company wants secure communication with its employees, the employees should use a reliable VPN for their mobile to connect to the company's VPN. That can prevent attackers from infiltrating the session. Another layer of defense is obtained with appropriate app installation, e.g., the Trustd mobile, which will check a potential victim's local WiFi connection for MITM activity and alert it. The business-focused Traced solution simultaneously informs the company's IT administrator, who should ensure secure communication. Although the protection against MITM is crucial, only 8% of companies in 2021 took technical measures to protect employees from risky Wi-Fi connections. According to a survey, over 20% of companies experienced a mobile device breach in 2020-2021. (Verizon, 2021 Mobile Security Index, 2021)

5 MANAGING MITM PROTECTION

In 2019, 11% of companies reported being affected by MITM attacks, according to the Fortinet State of Operational Security Report 2020 (Fortinet, 2020). As a protective measure against MITM attacks, 27% of websites were using HTTP Strict Transport Security (HSTS) as of December 11, 2023. (W3Techs, 2023) Additionally, according to Verizon (2023), 7% of users did not take any measures to protect their home Wi-Fi.

According to a survey by Enterprise Management Associates, close to 80% of internet TLS certificates are vulnerable to MITM attacks, with 25% of all certificates having already expired (Goldstein, 2023).

After the COVID-19 pandemic, many employees continue to work hybrid schedules and potentially use unsecured public Wi-Fi networks. They remain vulnerable to MITM attacks. There are ways one can try defending himself without knowing about MITM attacks in detail. A good idea is to check if the lock symbol exists in the address bar. When analyzing how to prevent MITM attacks, the best are often the most basic cybersecurity tools. They include (Poremba, 2022):

- Firewalls and VPNs.
- SSL and security certificates.
- Multi-factor authentication to control access.
- Employing hardline connections for sensitive devices to critical networks.
- Deploying endpoint security to protect IoT devices directly.

Institutions, companies, or cities can offer public Wi-Fi but separate it from the internal networks, which should use strong-wired equivalent privacy (WEP) and Wi-Fi-protected access (WAP). WEP/WAP encryption can help prevent attackers from attacking.

Every user should use the Internet by (Gregg, 2015), (Martens, 2023), (Microsoft, 2023):

- using security defaults to improve identity security. For additional control, users can define conditional risk-based access policies.
- continuous access evaluation implementation.
- installing antivirus software that can block MITM malware and monitor networks, browsers, firewalls, dark web, etc.
- encrypted connections use.
- avoiding free and unsafe Wi-Fi hotspots for sensitive transactions.
- avoiding HTTP websites, using only the encrypted version of websites, and installing a browser plugin like "HTTPS Everywhere."

[4] IMSI - International mobile subscriber identity, a unique number that identifies the device owner through its SIM card.

- using a home Wi-Fi router with WPA2 encryption and resetting the default password to a strong one.
- not visiting websites when the browser warns about a site's certificate problem.
- updating the operating system, applications, and antivirus on all used devices.
- using a dedicated laptop for online banking.
- setting up two-factor authentication on all accounts if possible.
- continuous monitoring accounts for any suspicious or anomalous activity (for example, location, ISP, user agent, and use of anonymizer services).

Almost half of all security breaches occur due to human behavior. Therefore, organizations need to consider the human aspect when educating their staff on preventing MITM attacks. Security awareness training that aims to prevent MITM attacks should cover the following topics (Poremba, 2022):

- Why should users avoid public and open
- Wi-Fi networks?
- Why the use of secure websites (HTTPS) is a necessity?
- How to spot fake websites?
- How to avoid phishing scams?

However, to prevent MITM attacks, education is not sufficient. The policy measures need to be implemented. The MSI[5] showed that (Poremba, 2022):

- around one-half (52%) of organizations do anything to enforce their policy measures.
- 8% of organizations do not use a VPN when using public Wi-Fi.
- nearly one-half (46%) of VPN clients are out of date or misconfigured.
- Less than one-third of organizations (32%) ban the use of public Wi-Fi.

When any identity compromise appears, the first measure is to reset the password. However, when the sign-in session is compromised in AITM attacks, only a password reset is not an efficient solution. Even if the victim's password is reset and sessions are revoked, the attacker can set up persistence methods to sign in a controlled manner by tampering with MFA. An attacker can add a new multi-factor authentication (MFA) policy to gain control over a victim's account. This can be achieved by signing in with a one-time password (OTP) sent to the attacker's mobile phone. Despite the victim's actions taken, the attacker will still have control over the account. Although AI-powered threat management systems attempt to avoid MFA, it remains crucial for ensuring identity security. MFA is highly effective in preventing most threats. MFA forces AITM attackers to develop session cookie theft techniques. Organizations need to work with their identity provider to ensure security controls like MFA. Microsoft customers can implement methods like using the Microsoft Authenticator, FIDO2 security keys, and certificate-based authentication (Microsoft, 2023).

6 CONCLUSION

The ways of using computers and networks are changing, the number of users is growing, but so is the number of malicious users who want something that does not naturally belong to them. In parallel with the development of new user software, programs for system protection and attacks on systems are also being developed. Each new software brings with it new risks. Both hackers and security experts are actively looking for potential vulnerabilities. The only question is who will be faster at a certain moment.

Based on the analysis, we saw that MITM attacks did not arise with the advent of computers and computer networks. They have existed since ancient times. Also, this analysis showed that they can cause extensive damage to users, service providers, and everyone who uses the Internet. Methods for performing MITM attacks change over time. Nowadays, more and more knowledge and often advanced technology is required. There are MITM attacks on individual users and large corporations.

Often, MITM attacks are combined with other types of attacks, so it is difficult to draw a line and classify an individual attack into a certain category. Many attacks included MITM attack elements.

[5] MSI – Verizon's 2022 Mobile Security Index

After analyzing various examples, we found that large MITM attacks still occur and have not yet been overcome. Therefore, we reject the null hypothesis and accept the alternative hypothesis that states "MITM attacks still exist and can cause harm to modern computer systems and their users".

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

Antonioli, D. (2023). BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 636-659). Copenhagen: ACM.

Arndt, J. (2023, May 09). *Man-in-the-Middle (MitM) attacks reaching inboxes increase 35% since 2022.* Retrieved from Cofense: https://cofense.com/blog/cofense-intelligence-strategic-analysis-2/?utm_source=bambu&utm_medium=social&utm_campaign=advocacy&blaid=4531672

Ashford, W. (2018, May 15). *No need to panic about Efail attacks*. Retrieved from ComputerWeekly: https://www.computerweekly.com/news/252441102/No-need-to-panic-about-Efail-attacks

Case No. 5:16-MD-02752-LHK, U. S. (2020, Mar 06). *Yahoo! Inc. Customer Data Security Breach Litigation Settlement. Case No. 5:16-MD-02752-LHK .* Retrieved from Yahoodatabreachsettlement: https://yahoodatabreachsettlement.com/

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017, 07 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

CISA. (2016, Sep 30). *Lenovo Superfish Adware Vulnerable to HTTPS Spoofing.* Retrieved from Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/news-events/alerts/2015/02/20/lenovo-superfish-adware-vulnerable-https-spoofing

Ecuron. (2023). *Man In The Middle Attack (MITM) – A Primer*. Retrieved from Ecuron: https://www.ecuron.com/man-in-the-middle-attack-mitm-a-primer/

EFAIL. (2018, May 16). Retrieved from EFAIL: https://efail.de/

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

Fortinet. (2020). *2020 State of Operational Technology and Cybersecurity Report.* Fortinet. Retrieved from https://www.arrow.com/ecs-media/10918/report-2020-ot-cybersecurity.pdf

Goldstein, P. (2023, Oct 13). *How To Detect and Prevent 'Man in the Middle' Attacks.* Retrieved from BizTech.

Goodin, D. (2015, Feb 19). *Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated].* Retrieved from ars Technica: https://arstechnica.com/information-technology/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

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

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

Henriques, N. (2016, Dec 19). *1-Billion Yahoo Users' Database Reportedly Sold For $300,000 on Dark Web.* Retrieved from Linkedin: https://www.linkedin.com/pulse/1-billion-yahoo-users-database-reportedly-sold-300000-nuno-henriques

Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2023). *2023 Data Breach Investigations Report.* Verizon. Retrieved from Verizon.

Hypr. (2023). *Adversary-in-the-Middle (AitM)*. Retrieved from HYPR: https://www.hypr.com/security-encyclopedia/adversary-in-the-middle

Irei, A., & Scarpati, J. (2022, Dec 06). *Wireless security: WEP, WPA, WPA2 and WPA3 differences.* Retrieved from TechTarget: https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

Jasek, S. (2016, Jul-Aug). GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy. *Black Hat USA 2016* (p. 49). Mandalay 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

Khandelwal, S. (2016, Dec 15). *Yahoo Admits 1 Billion Accounts Compromised in Newly Discovered Data Breach.* Retrieved from The Hacker News: https://thehackernews.com/2016/12/yahoo-data-breach-billion.html

Kiprin, B. (2021, Apr 02). *What Is the Heartbleed Bug and How to Prevent It.* Retrieved from VeraCode: https://crashtest-security.com/prevent-heartbleed/

Martens, B. (2023, Jun 07). *What Is a Man-in-the-Middle Attack? [Full Guide 2023]*. Retrieved from Safety Detectives: https://www.safetydetectives.com/blog/avoiding-the-man-in-the-middle-preventing-a-common-cyberattack/

Microsoft. (2023, Jun 08). *Detecting and mitigating a multi-stage AiTM phishing and BEC campaign*. Retrieved from Microsoft: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

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

Perlroth, N. (2017, Oct 03). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Poddebniak, D., Dresen, C., Mueller, J., Ising, F., Schinzel, S., Friedberger, S., . . . Schwenk, J. (2018). Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels. *27th USENIX Security Symposium* (pp. 549-566). Baltimore: USENIX.

Poremba, S. (2022, Sep 08). *How to prevent man-in-the-middle attacks in healthcare.* Retrieved from Verizon: https://www.verizon.com/business/resources/articles/s/how-to-prevent-man-in-the-middle-attacks-in-healthcare/

Proofpoint. (2016, Dec 13). *Home Routers Under Attack via DNSChanger Malware on Windows, Android Devices.* Retrieved from Proofpoint: https://www.proofpoint.com/us/blog/threat-insight/home-routers-under-attack-dnschanger-malware-windows-android-devices#

Rocha, E. (2018, Oct 1). *GhostDNS: New DNS Changer Botnet Hijacked Over 100,000 Routers.* Retrieved from GlobalDots: https://www.globaldots.com/resources/blog/ghostdns-new-dns-changer-botnet-hijacked-over-100000-routers/

Rowe, B. (2023, Sep 14). *The Latest Phishing Trends and Predictions*. Retrieved from Securus Communications: https://securuscomms.co.uk/the-latest-phishing-trends-and-predictions/

Senouci, F. z. (2023, Jul 23). *Yahoo Data Breach: An In-Depth Analysis of One of the Most Significant Data Breaches in History.* Retrieved from Medium: https://shellmates.medium.com/yahoo-data-breach-an-in-depth-analysis-of-one-of-the-most-significant-data-breaches-in-history-ba5b46be560b

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/

Stockley, L. (2021, Nov 22). *MitM Attacks: How to Avoid the Mobile Piggy in the Middle.* Retrieved from Traced: https://traced.app/2021/11/22/mitm-attacks-how-to-avoid-the-mobile-piggy-in-the-middle/

Sullivan, N. (2021, Mar 27). *Heartbleed Revisited.* Retrieved from Cloudflare: https://blog.cloudflare.com/heartbleed-revisited/

Toulas, B. (2023, Nov 28). *New BLUFFS attack lets attackers hijack Bluetooth connections.* Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/new-bluffs-attack-lets-attackers-hijack-bluetooth-connections/

Tran, S. (2017, Feb 21). *Verizon and Yahoo amend terms of definitive agreement.* Retrieved from Verizon News Center: https://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement

Vailshery, L. S. (2023, Jul 27). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. Retrieved from Statista: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Vanhoef, M., & Piessens, F. (2017). *Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse.* Retrieved from Krackattacks: https://www.krackattacks.com/

Vanhoef, M., & Ronen, E. (2019, Apr). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *IEEE Symposium on Security and Privacy.* Oakland (San Francisco): IEEE. Retrieved from https://wpa3.mathyvanhoef.com/

Venter, S. (2023, Mar 22). *Why your servers can still suffer from (a) Heartbleed – and what to do.* Retrieved from TuxCare: https://tuxcare.com/blog/why-your-servers-can-still-suffer-from-a-heartbleed-and-what-to-do/

Verizon. (2021). *2021 Mobile Security Index.* Verizon. Retrieved from Verizon: https://www.verizon.com/business/resources/reports/mobile-security-index.html

Verizon. (2023). *2023 Mobile Security Index white paper.* Verizon. Retrieved from https://www.verizon.com/business/resources/reports/mobile-security-index-report.pdf

Vijayan, J. (2019, Apr 08). *'Exodus' iOS Surveillance Software Masqueraded as Legit Apps*. Retrieved from DarkReading: https://www.darkreading.com/cyberattacks-data-breaches/-exodus-ios-surveillance-software-masqueraded-as-legit-apps

W3Techs. (2023, Dec 11). *Usage statistics of HTTP Strict Transport Security for websites.* Retrieved from W3Techs Web Technology Surveys: https://w3techs.com/technologies/details/ce-hsts

Zadig, S. (2012-2013, Fall/Winter). Botnet Investigations: An Inspector General Perspective. *The Journal of Public Inquiry*, 38-42.

Received for publication: 21.01.2024
Revision received: 08.02.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Cekerevac, Z., Cekerevac, P., Prigoda, L., & Naima, F. A. (2025, 01 15). Security Risks from the Modern Man-In-The-Middle Attacks. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 34-51. doi:10.12709/mest.13.13.01.04

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

Cekerevac, Zoran, Petar Cekerevac, Lyudmila Prigoda, and Fawzi Al Naima. "Security Risks from the Modern Man-In-The-Middle Attacks." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 34-51.

Style – **GOST** *Name Sort:*

Cekerevac Zoran [et al.] Security Risks from the Modern Man-In-The-Middle Attacks [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 34-51.

Style – **Harvard** *Anglia:*

Cekerevac, Z., Cekerevac, P., Prigoda, L. & Naima, F. A., 2025. Security Risks from the Modern Man-In-The-Middle Attacks. *MEST Journal,* 15 01, 13(1), pp. 34-51.

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

Security Risks from the Modern Man-In-The-Middle Attacks. **Cekerevac, Zoran, et al.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 34-51.