

A New Approach to Disabling SSL/TLS: Man-in-the-Middle Attacks are still Effective

Keiichiro Kimura
Kobe University, Japan
k_kimura@stu.kobe-u.ac.jp

Yoshiaki Shiraishi
Kobe University, Japan
zenmei@port.kobe-u.ac.jp

Masakatu Morii
Kobe University, Japan
mmorii@kobe-u.ac.jp

Abstract—Captive Portals have been implemented with the widespread adoption of public Wi-Fi to ensure appropriate network usage and protect it from malicious users. A Captive Portal is a mechanism that restricts or limits external communication until tasks such as user authentication or registration are completed when a device connects to the network. Under certain acceptable conditions, this paper proposes a new Man-in-the-Middle (MitM) attack that exploits this Captive Portal to circumvent SSL/TLS communication, enabling eavesdropping and tampering with communication content.

While many existing studies have discussed methods of eavesdropping and tampering with communications using Captive Portal as a starting point, the technique proposed in this paper is novel as it focuses on the screen transition behavior after authentication within the Captive Portal to initiate the MitM attack. Furthermore, our proposed method does not require specific constraints on the victim's device or its operating system, putting virtually all devices using public Wi-Fi at risk. Additionally, an attacker can carry out the attack using only the tool developed in this study and an Access Point equipped with Captive Portal functionality, making implementation straightforward.

To demonstrate the effectiveness and practicality of this attack method, we conducted evaluation experiments on various HTTPS-enabled websites in live operation. As a result, we confirmed that the attack proposed in this paper can successfully circumvent SSL/TLS communication without detection by the victim, enabling eavesdropping and tampering with communication content.

Index Terms—Wireless LAN, Public Wi-Fi, Man in the Middle, SSL/TLS, HTTPS

I. INTRODUCTION

Public Wi-Fi, while undoubtedly convenient, has undergone extensive scrutiny due to the inherent security threats it poses. These risks encompass the potential for malicious entities to eavesdrop on communications and the looming danger of unauthorized access. In response to these apprehensions, SSL/TLS communication has emerged as a recommended countermeasure. SSL/TLS involves the encryption and exchange of data, making it a crucial safeguard. In the present landscape, SSL/TLS has become the standard for the secure exchange of confidential information, significantly enhancing communication security. Furthermore, to address the vulnerabilities inherent to public Wi-Fi networks, various protective measures have been integrated, with the Captive Portal emerging as a prominent example. This innovative feature enables user authentication on public Wi-Fi networks, effectively curtailing the potential for illicit exploitation.

This paper presents a pioneering MitM (Man-in-the-Middle) attack that leverages the Captive Portal of public Wi-Fi networks to compromise SSL/TLS communication. Unlike conventional MitM attack techniques, such as downgrading HTTPS to HTTP or deploying counterfeit DNS and self-signed certificates, which have become progressively harder to execute due to the widespread implementation of HSTS and rigorous SSL certificate verification, the proposed MitM attack described herein solely hinges on the victim's use of public Wi-Fi. This method is notably straightforward to implement and is not confined by device type or operating system, rendering it a versatile avenue for exploitation. Furthermore, the proposed attack adeptly subverts encryption, HSTS, and Secure Cookie attribute assignment for the victim's visited sites capitalizing on the Captive Portal to obstruct legitimate SSL/TLS communication.

Additionally, this paper includes a hands-on demonstration of the proposed method, complemented by a subsequent evaluation. By emulating real-world conditions, we executed the MitM attack on several websites configured for HTTPS, conclusively substantiating the tangible threat posed by this method. Remarkably, this attack enabled communication interception without circumventing SSL/TLS, evading conspicuous alerts or broken elements on the victim's device.

The paper's structure unfolds as follows: Chapter II provides an overview of the landscape of public Wi-Fi threats and surveys pertinent research. Chapter III delves into the intricacies of the proposed method, while Chapter IV elaborates on its implementation and subsequent evaluation. In Chapter V, the method is examined from three perspectives: 'realistic threat,' 'comparison with related work,' and 'distinctions from phishing.' Chapter VI outlines effective countermeasures against the proposed method, and in Chapter VII we discuss considerations for research ethics. Finally, Chapter VIII concludes the study's findings.

II. BACKGROUND AND RELATED WORK

In this section, we first provide an overview of public Wi-Fi and the Captive Portal that are implemented in them. Then, we discuss the risks of MitM attacks against SSL/TLS exploiting public Wi-Fi and the security risks associated with captive portals, referencing related work.

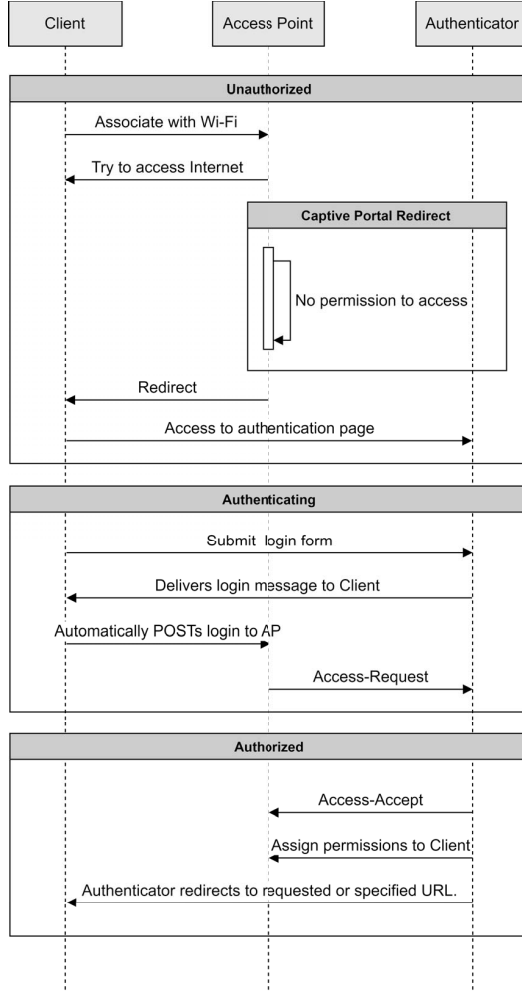


Fig. 1. Sequence diagram of Captive Portal workflow

A. Overview of Public Wi-Fi

Public Wi-Fi refers to the free Wi-Fi networks provided in public places. Nowadays, public Wi-Fi is widely prevalent, and the global economic value of Wi-Fi, developed by Telecom Advisory Services for Wi-Fi Alliance, is estimated to be 3.3 trillion dollars, including public Wi-Fi [14]. The number of installations, if limited to public Wi-Fi, is estimated to have reached over 1.2 million locations in Japan and approximately 18.6 million locations in the USA as of 2021 [14]. Considering this background, the need for user authentication functionality for public Wi-Fi inevitably arises. Captive Portal serves as one of the solutions to fulfill this role.

B. Overview of Captive Portal and its Significance

Captive Portal refers to the webpage to which unauthenticated users are redirected when they try to access the Internet from a browser, or the mechanism for this [5]. Fig.1 shows an example of the authentication flow using Captive Portal. The requirements associated with user authentication vary

depending on the network operator, but generally, they may involve the provision of social networking service (SNS) account information or email addresses, or agreement to terms of use. Familiar examples include the public Wi-Fi provided by cafes, airports, and public transportation, some of which use Captive Portals. Administrators of public Wi-Fi networks with Captive Portals typically specify the website to which users are redirected after authentication. For example, a café offering public Wi-Fi might specify its official website or an advertisement as the redirect destination. This could be a relatively familiar experience.

The significance of Captive Portal mainly lies in two aspects: 'Authentication' and 'User Information Collection'. Below, We explain these aspects.

- *The significance of 'Authentication'*: Normally, public Wi-Fi without authentication cannot identify the details of users. Such public Wi-Fi has the potential to become an infrastructure for committing misconduct such as posting criminal threats on anonymous bulletin boards or engaging in illegal downloads. Therefore, by introducing authentication through Captive Portal, there is a possibility that the actual perpetrators can be identified if any wrongdoing occurs.
- *The significance of 'User Information Collection'*: For example, when SNS authentication is adopted as a method of authentication for Captive Portal, companies providing public Wi-Fi can obtain information such as users' birth dates and purchasing-related information in exchange for offering free Wi-Fi to users. In this way, both public Wi-Fi and Captive Portal bring various benefits to both the user and the service provider.

However, these public Wi-Fi and Captive Portals are fraught with various security threats. The specifics of these threats are explained in the following sections, citing related work.

C. MitM attacks exploiting public Wi-Fi

Public Wi-Fi can serve as a catalyst for MitM attacks. This section introduces the concept of MitM attacks, with a particular focus on those that can be realized in a public Wi-Fi environment, by citing related work.

1) *SSL Stripping Attack*: In 2009, the SSL Stripping attack proposed by Moxie Marlinspike [8] became a major impetus for revisiting HTTP security protocols. The SSL Stripping attack is a type of MitM attack against SSL/TLS communications, where the attacker intercedes in the communication between the client and the server using ARP spoofing. In this attack, communication between the attacker and the server is performed over HTTPS, while communication between the attacker and the client occurs over HTTP, enabling the attacker to eavesdrop on the communication. As a countermeasure to this MitM attack, HSTS (HTTP Strict Transport Security) was established as RFC6797 in 2012 [9]. Since then, SSL Stripping attacks have become impossible against sites that have HSTS settings.

2) *Setozaki-Matsuo Attack*: As an extension of the SSL Stripping attack, in 2016, Takashi Setozaki and his research team proposed an SSL Stripping attack that bypasses measures taken by HSTS [15]. This attack method involves the attacker rewriting links in communication with the victim to domains not on the HSTS list, thereby bypassing HSTS and forcing HTTP communication between the victim and the attacker. This attack method is referred to as the Setozaki-Matsuo Attack henceforth. In 2019, Shouei Ou and his research team conducted an investigation into the threat level of this Setozaki-Matsuo Attack [16]. The Setozaki-Matsuo Attack is unsuccessful when the website is Always-On SSL (AOSSL). Shouei Ou and his team examined the proportion of domains that would be affected by the Setozaki-Matsuo Attack under this condition, targeting the top 500 .JP domains from the tranco-list [17] as of June 9, 2019. As a result, they found that 86% of the domains would not be affected by the Setozaki-Matsuo Attack, meaning they are domains where the Setozaki-Matsuo Attack would not succeed. Therefore, it can be said that the implementation of the Setozaki-Matsuo Attack is currently difficult.

D. Security Risk of Captive Portal

Captive Portals inherently pose various security risks due to their nature of allowing access to an operator-specified site in order to meet network access requirements imposed by network operators. This section introduces several related words discussed in relation to the security risks of Captive Portals.

1) *The risk of being tracked for browsing behavior*: Suzan Ali and others conducted a study on the behavior of web tracking and data collection targeting a unique public Wi-Fi in Montreal, Canada [1]. As a result, it was revealed that collection of personal data related to privacy and persistent third-party tracking cookies were used to track users' browsing behavior through the Captive Portal site.

2) *The risk of session hijacking*: Captive Portals also potentially enable session hijacking attacks. A research team led by Haidong Xia at the University of Pittsburgh has experimentally demonstrated that session hijacking and freeloading attacks are possible through the act of Captive Portals allowing clients access to the Internet [2].

3) *The risk of malicious components to boot*: A research team led by Vineeta Jain at the Malaviya National Institute of Technology in Jaipur has proposed a D2D (Device To Device) attack exploiting Evil Twin and Captive Portal [3]. The details of the attack presuppose that a benign app with a malicious component embedded by a malicious third party is pre-installed on the victim device, and the component is activated through the authentication action of the Captive Portal, and it is an exploit in which a certain device starts malicious activities on the victim device via a wireless communication channel. The authors argue that this attack has the potential to install a backdoor on the victim device or leak confidential information to a malicious server.

4) *The risk of MitM attack*: The most threatening risk would be a MitM attack initiated by a Captive Portal. Hiroshi TOKUMARU has demonstrated a MitM attack in his article, assuming a public Wi-Fi that has introduced a Captive Portal [4]. Specifically, it is a method where a malicious third party prepares a fake AP, pastes a bank account link in the fake site that is redirected after Captive Portal authentication, and extracts confidential information by setting up a MitM using Burp Suite [7]. While this attack can be avoided by websites setting HSTS, it is feasible and the realistic threat is quite large.

As can be seen, the security risks associated with, or originating from, Captive Portals are diverse.

III. MITM ATTACK AGAINST SSL/TLS COMMUNICATION USING CAPTIVE PORTAL

In this section, we propose a new MitM attack using Captive Portal to disable SSL/TLS communication. The main feature of this attack is that it disables SSL/TLS communication. In other words, even if the legitimate server had applied HSTS or Secure Cookie attributes to the HTTP Header, they would be meaningless. In the following, we first state the assumptions for the MitM attack we propose. Next, we present the attack model for the MitM attack. Finally, we explain the system model of the tools that the attacker uses to realize the MitM attack.

A. Assumptions

Let's assume a scenario in a location where public Wi-Fi is available (e.g., cafe, school, enterprise), with an Access Point (AP) characterized as follows:

- *A malicious third party has installed a fake AP that masquerades with the SSID of the legitimate AP*: This can easily be achieved by capturing the beacon of the legitimate AP, acquiring its SSID, and setting it in the administrator console of the fake AP. Here, *legitimate AP* is defined as *an AP provided and installed by official services or institutions*.
- *The fake AP uses a Captive Portal to permit internet access*

Furthermore, we make the following assumptions for users utilizing public Wi-Fi:

- *They use their smartphone or their laptop*
- *They do not verify the destination of their internet communication*: According to a study on public Wi-Fi security risk awareness by Abdulkader et al. [6], it was revealed that approximately 85% of the survey participants were not fully aware of the risks of fake APs, phishing attacks, and MitM attacks lurking in public Wi-Fi. Furthermore, considering that phishing attack is still one of the most common cyber attacks, it's reasonable to assume that the average user does not check the destination every time they browse the web. Hence, the this assumptions are sufficiently plausible.

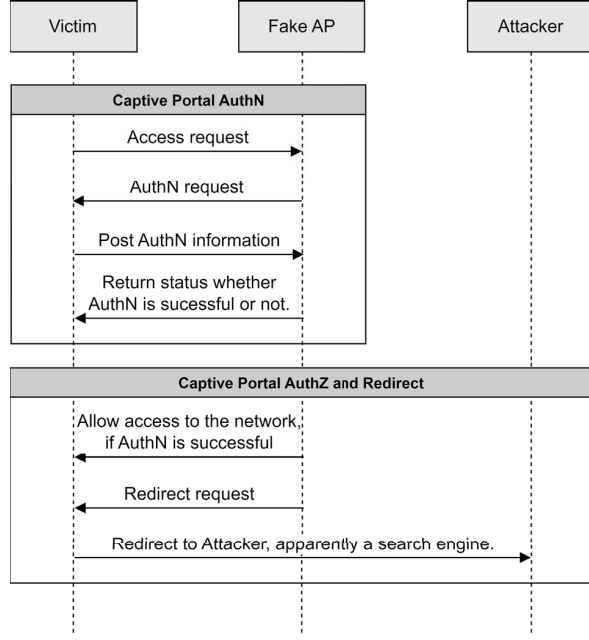


Fig. 2. Sequence diagram of setting up the Captive Portal

B. Attacking Model

Here, we describe the proposed attack model step by step.

1) *Setting up the Captive Portal*: As stated in III-A, we assume that the fake AP can be configured with a Captive Portal. As mentioned in II-D, Captive Portal has a characteristic that allows it to redirect users to a site specified by the provider after authentication. Generally, public Wi-Fi providers configure their company site or promotional sites as the destination sites. One motive for using public Wi-Fi is internet surfing, but users usually do not start surfing from the redirected company site. Typically, they reach the site they want to browse from the search engine screen provided by their web browser. Therefore, in this proposed method, the site to redirect to after authentication with Captive Portal is set to a fake search engine (such as Chrome, Safari, Edge) prepared by the attacker. (Fig.2)

2) *Initiating MitM Attack from the Redirected Site*: If the victim starts internet surfing from the fake search engine, all search keywords (hereafter referred to as queries) are secretly passed to the attacker. Using these obtained queries, the attacker retrieves search results from a legitimate search engine and modifies some of the hyperlinks in those results to point to a domain hosted by the attacker, and presents these results to the victim. To achieve this, the attacker may prepend the string '/template?q=' to the hyperlinks. Here, 'template' refers to the endpoint on the server where the attacker is waiting, and 'q=' refers to the query that is awaited at that endpoint. For example, by making the URL 'https://example.com' into '/template?q=https://example.com', the victim's request is sent to the attacker, revealing the URL of the site that the victim wants to view. (Fig.3)

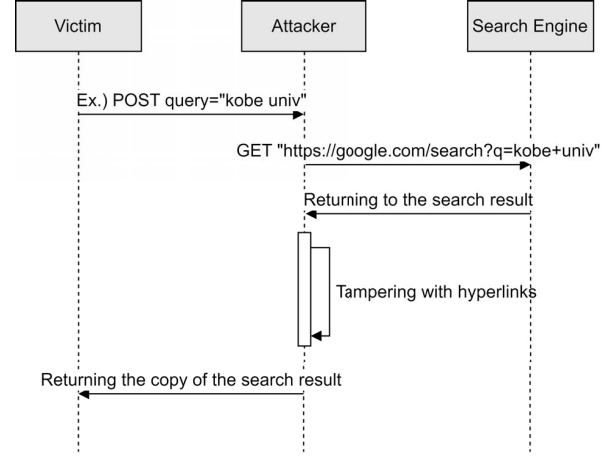


Fig. 3. Sequence diagram of initiating MitM attack from the redirected site

3) *Eavesdropping and Tampering with Communication via MitM Attack*: From the search results, the victim selects the site they wish to browse. As previously mentioned, the selected site's domain has been secretly altered by the attacker, so the URL of the site the victim wants to browse can be entirely captured by the attacker. The attacker then queries the legitimate web server using this URL, obtains the access result, alters the hyperlinks, and presents them to the victim. In this way, the communication between the victim and the web server is completely mediated by the attacker, making eavesdropping on the content possible. Additionally, tampering with the content is also feasible, just like altering the hyperlinks. This becomes the most threatening when the victim operates on sites that manage personal accounts, such as e-commerce sites or online banking, through the attacker. In such cases, all confidential information, including login details, would be handled through the attacker, causing all sensitive information to leak to the attacker. (Fig.4)

This concludes the attack model of the proposed method.

C. System Model

In this research, we implemented an attack tool to realize the proposed method. Details of the implementation of the attack tool are explained later, but here, we describe the system model of the implemented attack tool. The implemented attack tool is composed of the architecture shown in Fig.5 and performs its functions through the interrelationship of multiple modules. Below is the description of each module.

- *Router Module*: This module manages endpoints and routes requests from victims. After routing, it passes the content of the request to the Handler Module.
- *Handler Module*: From the content of the request passed by the Router Module, this module extracts information such as parameters entered by the victim and URLs of websites the victim wants to access, and passes them to the Usecase Module.

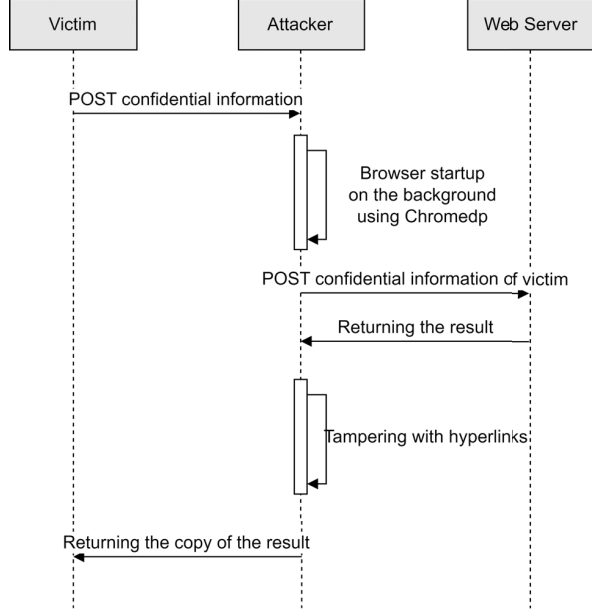


Fig. 4. Sequence diagram of eavesdropping and tampering with communication via MitM attack

- **Usecase Module:** This module performs the necessary processes for the parameters passed from the Handler Module. Specifically, it accesses the web server, sends requests, and retrieves the responses. It also properly replaces hyperlinks so that the victim's request will go through the attacker's server. Then, it automatically generates HTML files with these processes applied to the Template Module.
- **Template Module:** This module manages the HTML files to be presented to the victim.
- **Symbols Module:** Before being automatically generated as HTML files in the Template Module, this module manages the strings and symbols that should be deleted or replaced from that HTML file. When the Usecase Module performs specific processes, it modifies and automatically generates the HTML files based on the information managed by this module.
- **Public Module:** In this module, management is carried out for image resources prepared in advance by the attacker, and image files to be managed when automatically generating HTML files. Basically, all image resources in automatically generated HTML files can be supplemented, but for example, image resources needed to create a fake search engine are managed in this Public Module.

This concludes the explanation of this system model.

IV. IMPLEMENTATION AND EVALUATION

In this section, we describe the demonstration experiment of the proposed method and its results.

TABLE I
EXECUTION ENVIRONMENT OF THE ATTACK TOOL

Device Name	OS
Surface Laptop 4	Windows10

TABLE II
DEVICE USED AS A FAKE AP

Device Name	OS
GL.iNet GL-AR300M(shadow)	OpenWrt

A. Implementation of the Attack Tool

This time, we actually implemented the attack tool described in III-C. The implementation was done using Go 1.17, and external packages such as chromedp (v.0.7.7) [18] provided by Chromedp and cdproto (v0.0.0-20220131204822-e6abebe7b8cd) [19] were used. For other functionalities, only the built-in packages were used for implementation.

B. Introduction of Experimental Devices

The environment for executing the attack tool used a Surface Laptop 4 (TableI). The AP that the attacker used as a fake AP was GL.iNet GL-AR300M (shadow) (TableII). GL.iNet GL-AR300M (shadow) can be configured as an AP with a Captive Portal implemented, and the site to redirect to after authentication can be easily set from the admin panel. The victim devices used this time were a Surface Laptop 3 and Pixel 3 XL (TableIII).

C. Establishment of Evaluation Criteria

In conducting a demonstration experiment, we formulated evaluation criteria for the proposed method. Specifically, the following four criteria (Ev.1-4) were established:

- **Ev.1. Whether the website can operate without discomfort:** This criterion evaluates whether the proposed method can perform a MitM attack against SSL/TLS communication.
- **Ev.2. Whether confidential information can be obtained:** This criterion evaluates whether the proposed method can not only eavesdrop and tamper with communication content but also eavesdrop on highly confidential information.
- **Ev.3. Whether it can operate without explicit warnings:** This criterion evaluates whether the proposed method can be executed without being recognized by the victim.
- **Ev.4. Whether it can operate without explicit broken images:** Similar to 3, this criterion evaluates whether the proposed method can be executed without being recognized by the victim.

D. Experiment and Evaluation

This time, we conducted a demonstration experiment of the MitM attack using the proposed method on an actually

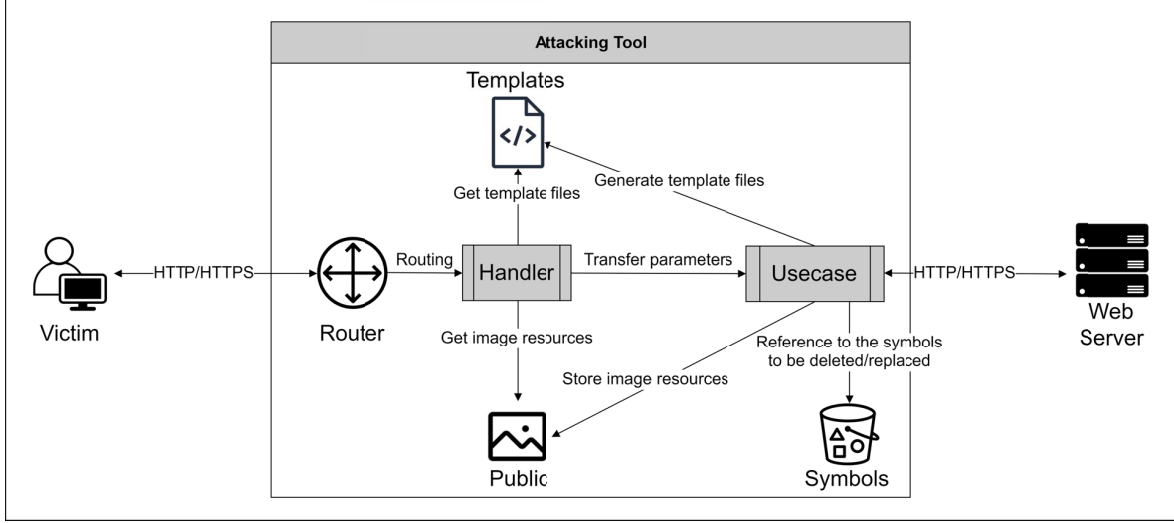


Fig. 5. Architecture of the implemented attack tool

TABLE III
DEVICES USED BY THE VICTIM

Device Name	OS
Surface Laptop 3	Windows10
Pixel 3 XL	Android 12

TABLE IV
DEMONSTRATION TEST RESULTS OF THE ATTACK AGAINST EC SITES

	HSTS	Cookie Secure	Ev.1	Ev. 2	Ev. 3	Ev. 4
EC Site A	Set	Set	✓	✓	✓	✓
EC Site B	Set	Not Set	✓	✓	✓	✓

operating e-commerce site. The reason for choosing an e-commerce site is that it is generally widely and frequently used, and often handles personal information. In this experiment, in consideration of research ethics and to prevent any disadvantage to third-party organizations, the details of the e-commerce sites are withheld.

The scenario of the experiment is as follows. First, the attacker sets up a fake AP and waits for the victim who wants to use the internet to connect. The victim who connects to the fake AP is required to authenticate using a Captive Portal before connecting to the internet. After authentication, the attacker redirects the victim to a fake search engine. The victim, not recognizing that the search engine is fake, follows the search procedure to enter the e-commerce site. Then, to log in to their personal account on the e-commerce site, the victim enters their authentication information on the login screen and actually logs in to use it.

The experimental results of this attack scenario are shown in TableIV. Ev. 1-4 refer to the respective evaluation criteria numbers. As a result of the experiment, we were able to enter personal accounts on actually operating e-commerce sites that

```

Login
method : GET
email : [REDACTED]@gmail.com
password: [REDACTED]

```

Fig. 6. The logs of the attack tool's CLI show the victim's credentials in plain text.

have been HTTPS and HSTS enabled, using the Captive Portal and the implemented attack tool.

All these communications were carried out through the attacker, and the attacker was able to eavesdrop on the content of the sites the victim was viewing, and the information needed for login, such as email address and password, in plaintext (Fig.6).

V. DISCUSSION

In this chapter, we delve into the proposed method by drawing upon the implementation details and outcomes from the evaluation experiments. The ensuing discussion is structured around three key perspectives: "Realistic security threats", "Comparison with related work", and "Difference from phishing." These visual aids serve to reinforce the forthcoming exploration of the proposed method.

A. Realistic security threats

This section examines the practical threat of the MitM Attack proposed in this paper. Specifically, we explore three key perspectives: "Feasibility," "Anticipated Security Threats", "Scope of Victims" and "Difficulty of Detection".

1) *Feasibility*: Let's assess the feasibility of the proposed method. The malicious third party only requires the attack tool demonstrated in the experiment, the Golang execution environment, and an Access Point (AP) with a Captive Portal. Specialized technology or tools are unnecessary. Furthermore, APs can be obtained inexpensively, making a MitM attack

potentially accessible to anyone. The only constraint on victims is their use of the attacker's malicious AP. Considering these factors, it is evident that the proposed method is easily achievable.

2) *Anticipated Security Threats*: Drawing from experimental results, several security threats pertaining to potential victims in this proposed method are outlined below:

Leakage of Confidential Information: The demonstration experiment successfully logged into an HTTPS-secured website handling account information through the attacker as an intermediary. Despite HTTPS, HSTS, and Secure Cookie attributes, victim data can still be leaked due to communication channeled through the Captive Portal. This implies a high risk of confidential information exposure even with robust security measures.

Eavesdropping and Tampering with Communication Content: The employed attack tool temporarily caches HTML, js, css, and images from the target website. Consequently, not only the victim's browsed content but also internal hyperlinks, text data, and js files can be dynamically altered. In summary, successful execution of this proposed method presents substantial security threats.

3) *Scope of Victims*: The potential victims encompass users who utilize the fake AP, authenticate the Captive Portal, and subsequently browse the web via the counterfeit search engine. This method's applicability is essentially independent of the victim's device (smartphone, notebook PC, etc.), operating system, version, or model. Consequently, any device employing a fake AP-driven user interface could be susceptible to the proposed method.

4) *Difficulty of Detection*: Given the experimental outcomes, recognizing an attack employing this proposed method is challenging for victims due to the following reasons:

Absence of browser warnings: In this approach, victims engage with the attacker upon public Wi-Fi authentication. Consequently, they do not communicate with the legitimate server offering the website while connected to the attacker via HTTP. SSL certificate manipulation or self-signed certificates are unnecessary, evading SSL certificate verification. This circumvention prevents browser warnings, concealing the middleman's presence.

Seamless display of fake site: The attack tool allows seamless communication between the attacker and the legitimate server, permitting the downloading of all website scripts and images post-rendering. Regardless of the website's rendering method, the attacker can mimic the site by appropriately modifying hyperlinks in the HTML file. This mimicking makes it arduous for victims to identify the attacker's presence.

Considering these three aspects, it is evident that the method introduced in this paper could indeed pose a significant real-world threat.

B. Comparison with related work

In this section, we delve into how the MitM attack proposed in this paper compares as a threat to the related work. As the method introduced in this study involves a MitM attack

against SSL/TLS communication using a Captive Portal, we primarily contrast it with the SSL Stripping attack, Setozaki-Matsuo Attack, and the MitM attack demonstrated by Hiroshi TOKUMARU utilizing a Captive Portal and Burp Suite.

1) *Comparison with SSL Stripping Attack*: As detailed in Section II-C, SSL Stripping attacks are impeded on websites with HSTS enabled. In contrast, our proposed method enables a MitM attack even on sites employing HSTS. This disparity arises because, following Captive Portal authentication, the victim's communication exclusively transpires with the attacker. Hence, our method widens the spectrum of websites vulnerable to MitM attacks.

2) *Comparison with Setozaki-Matsuo Attack*: Per Section II-C, research by Shouei Ou and colleagues underscores the limited impact of the Setozaki-Matsuo Attack. In conjunction with the SSL Stripping attack comparison, our method can execute a MitM attack despite a victim's browsing site having HSTS activated. Additionally, even if the victim is on a non-HSTS site, the Setozaki-Matsuo Attack can't initiate a MitM attack until it detects HTTP communication. In contrast, our proposed method can commence a MitM attack from the outset of web browsing. Therefore, our method's MitM attack presents a more potent threat than the Setozaki-Matsuo Attack.

3) *Comparison with Hiroshi TOKUMARU's Demonstrated Method*: Referencing Section II-D, Hiroshi TOKUMARU's experiment uses Burp Suite to extract online banking login data from a counterfeit site following Captive Portal authentication. This entails forcing victim-attacker communication into HTTP while converting attacker-bank communication to HTTPS, with the caveat that the site being communicated with must employ HSTS. Conversely, our proposed method's threat is rooted in invalidating HSTS settings, differentiating it from TOKUMARU's technique.

C. Difference from phishing

In this section, we elucidate distinctions between the MitM attack proposed in this paper and phishing attacks. According to research led by Zainab Alkhalil [10], the evolving nature of phishing attacks has precluded a definitive definition. Pish-Tank defines phishing as a "fraudulent attempt, usually made through email, to steal your personal information", while APWG characterizes it as a "criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials", according to [12]. Against this backdrop, we define and explore "phishing" as a "cyber attack that impersonates a reputable organization, presents a fake site link through email or SMS messages, and solicits the input of confidential information".

1) *Methodology Distinction*: The manner of directing users to counterfeit sites differs between phishing and the proposed method in the following ways:

- *Phishing*: Attackers in phishing endeavors provide users with fake website links, usually via emails or text messages. These links often masquerade as legitimate

websites, like banks or social networks, to capture login details.

- *Proposed Method:* Our approach employs a Captive Portal to divert users to a designated fake site, typically facilitated over networks like public Wi-Fi. When users connect to the network, they are redirected to the provider's Captive Portal page for authentication. If attackers impersonate this Captive Portal, they intercept all user data and browsing activities.

The mechanism for redirecting to counterfeit sites distinguishes this proposed method from phishing.

2) *Purpose Disparity:* Aims of phishing and the proposed method contrast in the following ways:

- *Phishing:* Phishing primarily seeks to pilfer user login and personal information.
- *Proposed Method:* The Captive Portal-based approach not only targets login data theft but also encompasses eavesdropping and tampering with communication content.

This encompasses more than just confidential information interception, setting it apart from phishing.

3) *Attack Starting Point Distinction:* Points of attack inception diverge between phishing and the proposed method as follows:

- *Phishing:* Phishing attacks start when users click on email links or accidentally access fraudulent websites.
- *Proposed Method:* The proposed method, using the Captive Portal, initiates attacks when users connect to networks like public Wi-Fi.

This fundamental difference in attack commencement distinguishes the two approaches.

In conclusion, the MitM attack proposed in this paper can be said to be different from phishing attacks in various aspects.

VI. COUNTERMEASURES

In this section, we address countermeasures against the MitM attack proposed in this paper. Specifically, we discuss countermeasures from three viewpoints: 'Website Providers', 'Public Wi-Fi Providers', and 'Public Wi-Fi Users'.

A. Countermeasures for Website Providers

As mentioned earlier, the distinctive feature of the proposed method lies in its ability to undermine the encryption of communication content through SSL/TLS and HSTS. Consequently, there appear to be limited specific and effective measures that website providers can adopt.

B. Countermeasures for Public Wi-Fi Providers

We outline and elaborate on countermeasures that public Wi-Fi providers could implement to thwart the proposed method:

- *Offering an AP Connection App:* Employing an AP connection app offers numerous advantages. In the context of the proposed method, this approach serves as a deterrent against users inadvertently connecting to fake APs. Given that the proposed method initiates by impersonating a

legitimate AP to induce erroneous connections, this countermeasure proves effective. However, challenges persist, such as development costs and the necessity for a securely designed app. These challenges pose potential obstacles to the adoption of an AP connection app.

C. Countermeasures for Public Wi-Fi Users

Outlined below are countermeasures that public Wi-Fi users can undertake to mitigate the risks posed by the proposed method, accompanied by explanations:

- *Closing Redirected Website Tabs:* The MitM attack realized by the proposed method involves evading SSL/TLS by transforming the website, redirected by the Captive Portal after authentication, into a counterfeit search engine. Nonetheless, if users close and remove the browser tab to which they were directed, the starting point of the MitM attack in the proposed method becomes nullified. It's important to note that merely closing the redirected website doesn't eliminate the threat, as the session could persist in the background. Thus, by thoroughly closing the browser tab, users can effectively neutralize the risk of a MitM attack.
- *Validating Communication Destinations:* The proposed method assumes that victims of the attack neglect to verify the legitimacy of their device's communication partners. Given the enduringly significant number of phishing attack victims [13] and the ongoing deficiency in awareness of security risks [6], this assumption holds merit. Nevertheless, the most efficacious means of detecting the proposed method is by confirming the communication destination. Consequently, if users possess a heightened awareness of potential security risks, this could serve as a potent countermeasure.

VII. CONSIDERATION FOR RESEARCH ETHICS

The purpose of this research is to investigate unknown threats in widely adopted technologies and to promote their countermeasures. This research has the potential to benefit a very broad range of end users. All evaluation experiments for the proposed method in this paper were conducted within the laboratory, and no attacks were carried out on real-world devices outside the laboratory.

To minimize the direct impact of this paper's publication, the source code for the attack tools implemented in this research is not disclosed at all. Also, to prevent any disadvantage to third-party organizations, details of the e-commerce sites targeted for MitM attacks are anonymized. Moreover, for the sake of demonstrating the fairness of the experiments, minimal information such as the type of devices and OS is disclosed.

VIII. CONCLUSION

In this paper, we introduce a novel MitM attack that exploits a Captive Portal to incapacitate SSL/TLS communications. Furthermore, we substantiate the tangible threat posed by our approach and underscore the effectiveness of countermeasures through compelling evidence of successful eavesdropping on

confidential data during MitM attacks on currently operational HTTPS-enabled websites. The innovative aspect of our method lies in its execution of a MitM attack via redirection to a counterfeit search engine post-Captive Portal authentication. This strategic maneuver allows us to circumvent SSL certificate verification and override HSTS settings. Notably, our method leverages the established protocol of the Captive Portal for MitM attacks, requiring no specific prerequisites related to the victim's device or its operating system. As a result, an extensive array of devices using public Wi-Fi becomes potentially vulnerable. Moreover, the implementation of our proposed method necessitates merely the utilization of the attack tool we developed in this study, a Golang execution environment, and an access point with Captive Portal functionality, rendering it exceptionally straightforward to deploy. While many methodologies proposed in related works can be countered by the application of HSTS or the attribution of Secure Cookie attributes, our method, by its ability to nullify these server-side configurations, emerges as a more formidable threat compared to existing MitM attack techniques.

ACKNOWLEDGMENT

This research was in part conducted under the '*Research and development on new generation cryptography for secure wireless communication services*' contract for the '*Research and Development for Expansion of Radio Wave Resources (JPJ000254)*', which was supported by the Ministry of Internal Affairs and Communications, Japan.

REFERENCES

- [1] Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr M. Youssef, "On Privacy Risks of Public Wi-Fi Captive Portals", *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019*, pp.80-98 (2019)
- [2] Haidong Xia, J. Brustoloni, "Detecting and Blocking Unauthorized Access in Wi-Fi Networks", *NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communication, Third International IFIP-TC6 Networking Conference*, pp.795-806 (2004)
- [3] Vineeta Jain, Vijay Laxmi, Manoj Singh Gaur, Mohamed Mosbah, "ETGuard: Detecting D2D attacks using wireless Evil Twins", *Elsevier Computer Security* 83 (2019), pp.389-405 (2019)
- [4] <https://qiita.com/ockeghem/items/c6a3602d2c2409f89fbb> (Accessed at 2023-08-15)
- [5] Wiederkehr, Patrick, "Approaches for simplified hotspot logins with Wi-Fi devices", *ETH, Swiss Federal Institute of Technology, Computer Science Department*, p.64 (2009)
- [6] Abdulkader, Mohamad, "Why do people use public Wi-Fi?: An investigation of risk-taking behaviour and factors lead to decisions", url: <https://his.diva-portal.org/smash/record.jsf?pid=diva2%3A1774094&dsid=2263> (Accessed at 2023-07-27)
- [7] Burp Suite, <https://portswigger.net/burp>
- [8] Moxie Marlinspike, "New Tricks For Defeating SSL In Practice", url: <https://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf> (Accessed at 2023-07-27)
- [9] RFC 6797, "HTTP Strict Transport Security (HSTS)", url: <https://datatracker.ietf.org/doc/html/rfc6797> (Accessed at 2023-07-27)
- [10] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, Imtiaz Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", *Frontiers in Computer Science* (2021)
- [11] PhishTank, "What is phishing?", https://www.phishtank.com/what_is_phishing.php?view=website&annotated=true (Accessed at 2023-07-27)
- [12] Anti-Phishing Working Group, "Phishing Activity Trends Report, 3rd Quarter 2018", url: https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf (Accessed at 2023-07-27)
- [13] Kaspersky, "The number of phishing attacks doubled to reach over 500 million in 2022", url: https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022 (Accessed at 2023-07-27)
- [14] Wi-Fi Alliance, "Global Economic Value of Wi-Fi 2021-2025", url: <https://www.wi-fi.org/file/global-economic-value-of-wi-fi-2021-2025> (Accessed at 2023-08-15)
- [15] Takashi Setozaki, Kazuto Matsuo, "An Enhanced Sslstrip Attack against HTTPS with HSTS", *Computer Security Symposium 2016*, pp.733-740 (2016)
- [16] Shouei Ou, Naoto Yanai, Takao Okubo, Shingo Okamura, "A study on sslstrip", *Computer Security Symposium 2019*, pp.1398-1405 (2019)
- [17] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, Wouter Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation", *Network and Distributed System Security Symposium* (2019)
- [18] Chromedp, "chromedp", <https://github.com/chromedp/chromedp> (Accessed at 2023-08-08)
- [19] Chromedp, "cdproto", <https://github.com/chromedp/cdproto> (Accessed at 2023-08-08)
- [20] Captive Portal, https://help.fortinet.com/fauth/5-1/Content/Admin%20Guides/5_1%20Admin%20Guide/400/406_Captive_portal.htm (Accessed 2023-08-15)