Hardening MFA web applications to counter evolving transparent phishinging attack vectors

Philipp Liermann 20-475873-20
Supervisor: Prof. Dr. Raad Bin Tareaf

February 4, 2024

Contents

1 Problem statement

These days most websites have implemented two or multi-factor authentication systems to prevent malicious third-party actors from using stolen login credentials to commit identity theft. Despite this, a new technique referred to as transparent proxy phishing still provides malicious actors the means to bypass two-factor authentication systems during social engineering based phishing attacks. This creates a critical security vulnerability, as this technique can be used to gain unauthorized access to otherwise secure systems. To resolve this issue, it is imperative to develop and implement effective measures to counteract transparent phishing and other methods of circumventing multi-factor authentication systems.

2 Research question

How can we protect multi factor authentication secured web applications from transparent proxy phishing attacks? Based on this question the following sub questions were derived:

- What exactly are classical phishing attacks in general and how do they differ from the new attack vector?
- How big is the threat imposed by this new type of phishing attack?
- Why are many organizations still not aware of this issue?
- What can be done to help developers counteract this type of security threat?

3 Objective

As credential theft and cyberfraud in general are still a growing problem in the digital age, it is important to develop and implement effective measures to counteract this threat. The objective of this thesis is to find and document different strategy's that can help organizations and developers to mitigate this new attack vector.

4 Theoretical foundations & current state of research

Cyberfraud is a form of internet-based fraud, usually involving the use of false identities and/or stolen information to illegally obtain money, property, or services. Cyberfraud is an increasingly pervasive problem that is becoming increasingly difficult to combat, as fraudsters become more sophisticated in their methods. In 2020, cyberfraud was estimated to cost the global economy over $6 trillion[1], with the financial sector suffering the most damages. The social, economic and reputational costs of cyberfraud can be incredibly damaging, and can range from the loss of money, to identity theft, to the disruption of businesses. Cyberfraud has become so pervasive that it is essential for businesses and individuals to take measures to protect themselves from it. This includes using strong passwords, using two-factor authentication, and staying up to date with the latest security protocols.

A phishing attack is a type of cyberattack in which an attacker attempts to gain confidential information, such as passwords, credit card numbers, or other sensitive information, by sending emails or other messages disguised as legitimate entities. These messages often include malicious links to faked login prompts that will steal the victims credentials upon entering them. These attacks are becoming increasingly sophisticated and difficult to recognize, making it important for everyone to remain vigilant and take steps to protect against them.

A HTTP reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. This type of proxy is sometimes referred to as a “gateway” or “tunneling” proxy because it acts as a gateway for the traffic to and from the server. A reverse proxy will typically receive a request from a client, then forward that request to an appropriate server on the same network. It then retrieves the response from the server and sends it back to the client. This type of proxy server is most often used in enterprise networks to protect against malicious traffic, to balance load between multiple servers, and to cache static content.

Transparent proxy phishing is a new technique used by attackers to intercept and steal multi-factor authentication (MFA) tokens from unsuspecting users. Instead of copying HTML code from the original page that the attacker is trying to impersonate, this new attack uses a HTTP reverse proxy to just redirect the users traffic to the original page. The attacking proxy operator can view and modify all traffic that is going through it while the victim sees a one by one copy of the original login page. By doing so login credentials and 2FA tokens can be extracted easily.

TLS is a cryptographic protocol that provides end-to-end security for data sent between a client and a server. It is widely used to secure web traffic, email, and other types of data. TLS is the successor to SSL, and is often referred to as SSL/TLS. If a webserver is using TLS its URL starts with the well known https:// prefix.

TLS Fingerprinting is a technique used to identify the TLS implementation of a client or server by analyzing the handshake process.

This can be used to identify which software is used by client or server. Industry standards for fingerprinting algorithms have existed for a long time. These include: JA3, JA3N and the whole JA4+ family.

Many scientific papers have been published on this topic, but there is still a lack of information on how to protect against this new attack vector. This is why it is important to find and document different strategies that can help organizations and developers to mitigate this new attack vector.

5 Research design

This thesis will be conducted in a quantitative research design. By analyzing existing literature and scientific papers on the topic, but also by running own experiments in which open source reverse proxy phishing toolkits will be used to setup attack simulations with the goal to find flaws in their attack implementation. With the gained knowledge from this experiments this paper will outline easy to follow strategies to protect web services from this threat.

6 Literature Review

6.1 Overview of Multi-Factor Authentication

Discuss the principles, types, and current adoption of MFA, highlighting its role in enhancing security.

6.2 Phishing Attacks: Evolution and Impact

Trace the evolution of phishing attacks from simple scams to sophisticated reverse proxy phishing, including case studies or statistics to underline their significance.

6.3 Existing Countermeasures

Review current strategies and technologies aimed at thwarting phishing attacks, particularly those targeting MFA systems, identifying their strengths and weaknesses.

The paper ”catching transparent phish” [**?**] provides a detailed analysis of the most used reverse proxy phishing toolkit and its potential to bypass MFA systems. The authors demonstrate how those toolkits can be used to intercept and steal MFA tokens, and propose a detection method based on a statistical model that evaluates a combination of TLS fingerprinting and response timing analysis. The authors provide a AI based solution for finding transparent phishing toolkits in the wild, but only provide limited advice on how to detect client connections of those toolkits on the server side.

7 Methodology

7.1 Research Design

Outline the research approach, whether qualitative, quantitative, or mixed methods, justifying the choice based on your research questions.

7.2 Data Collection

Describe how data will be gathered, including any experimental setups, simulations, or surveys planned.

7.3 Analysis Techniques

Detail the methods for analyzing the collected data, such as statistical analysis, content analysis, or software testing methodologies.

8 Experimentation

8.1 Simulation of Reverse Proxy Phishing Attacks

Describe the setup for simulating attacks, including the tools and environments used.

8.2 Evaluation of MFA Vulnerabilities

Explain how the simulations will be used to evaluate the vulnerabilities in current MFA implementations.

8.3 Testing of Countermeasures

Outline the process for developing and testing new or improved countermeasures against these attacks.

9 Results

9.1 Findings from Simulations

Present the data collected from the simulations, providing analysis and interpretation.

9.2 Effectiveness of Current Defenses

Assess the effectiveness of existing defenses against reverse proxy phishing based on your findings.

9.3 Proposed Solutions

Introduce any new solutions or improvements to existing solutions developed through your research.

10 Discussion

10.1 Implications of Findings

Discuss the broader implications of your findings for cybersecurity practices and MFA implementation.

10.2 Limitations and Future Research

Acknowledge any limitations of your study and propose areas for future research.

11 Literature Review

12 References

[1] Cybercrime Damages $6 Trillion By 2021 https://cybersecurityventures.com/annual-cybercrime-report-2017/

[2] Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits https://catching-transparent-phish.github.io/catching_transparent_phish.pdf

[3] Geo-Location based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack https://sci-hub.hkvisa.net/10.1145/2517881.2517889

[4] Analyzing 2FA Phishing Attacks and Their Prevention Techniques https://ieeexplore.ieee.org/abstract/document/9945766

[5] Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks https://www.sciencedirect.com/science/article/abs/pii/S2214212618300140

[6] Modlishka. Reverse Proxy https://github.com/drk1wi/Modlishka

[7] EvilNginx. Reverse Proxy https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/