Indian Institute of InformationTechnology Allahabad

SSL STRIPPING

Group Members:

Name	Roll Number
Shubham Netam	IIT2019028
Adelik Om Tyagi	IIT2019070
Nimish Upadhyay	IIT2019113
Ritik Parmar	IIT2019155
Jaidev Das	IIT2019197

Table of Contents

Abstract

SSL stripping is a serious crime and a serious threat, which is used by attackers to steal confidential and sensitive data. In this report we have mentioned its mechanism,working,ways to detect and prevent it. And also we have explained the practical implementation of SSL striping attack, SSL stripping Detection and SSL stripping Prevention technique.

Introduction

An SSL stripping attack is a type of cyber attack in which hackers downgrade a web connection from a more secure HTTPS to a less secure HTTP (HTTP and HTTPS are application protocols. HTTP transmits the data in plaintext whereas HTTPS sends data using a secure tunnel.). It prevents all communications from being encrypted and serves as a platform for man-in-the-middle attack, in which the hacker sits in the middle of a conversation to listen to or block information. This allows the hackers to see everything the user says in an unencrypted form.

Moxie Marlinspike ,an American computer security researcher,was the one who showed how one can bypass the security provided by HTTPS ,he demonstrated this for the first time at Black Hat Information security event,in 2009.

Every internet connection starts unsecured. Users must visit the website with the HTTP version before establishing authentication to visit the secure HTTPS version. These steps are intended to ensure confidentiality and to verify the legitimacy of those involved in the connection.

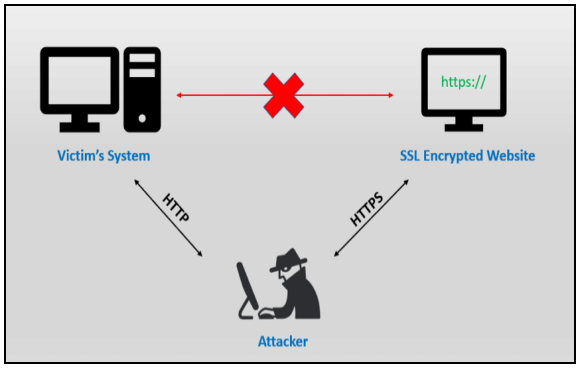
Hackers can strip the SSL connection by inserting themselves in the process. When they do, they act as an intermediary between establishing their own HTTPS connection with the Website (presenting as the user) and maintaining the HTTP connection with the User (pretending to be the Website). Once they have completed those connections, they can sit down in the middle of the conversation and simply accept everything the user submits to the website. When this happens, users can not only share information in plain text with an illegal source, but they can also get altered answers (because hacker communication can be retrieved from a legitimate website).

Mechanism and working of the SSL Stripping

Suffix ‘S’ in HTTPS represents SSL/TLS which is a secure and encrypted tunnel used for transferring and receiving sensitive data, where SSL stands for Secure Socket Layer and TLS stands for Transport Layer Security.Though TLS is a successor of SSL protocol it is commonly refer as “SSL”or ”SSL/TLS”.

Common scenario is :(i) Client sends an unsecure HTTP request, (ii) Server response through HTTP and redirects the Client to HTTPS, (iii) Then a secure connection between Client and Server is established.

There is an instance where the Client gets redirected from HTTP to HTTPS. Attacker intervenes in the redirection and uses this small window of opportunity to intercept connection between Client and Server.Then Attacker establishes a secure HTTPS connection with Server and an unsecure HTTP connection with Client. Performing a man-in the-middle attack using SSL stripping.



Source: www.venafi.com

Let say our Client wants to access his/her Instagram account and types www.instagram.com in the address bar. Attacker will first establish a connection with the client. Then the Attacker will forward the Client's request to Instagram's server and receive the HTTPS secure login page. Attacker is connected through https://www.instagram.com with sever and now Attacker has the control over the login page. Attacker demotes HTTPS to HTTP and sends to the Client browser. Client browser is redirected to http://www.instagram.com . Now Client's login credentials will be transferred in plain text, and the Attacker will obtain it. While the server will think it has secured connection with Client, which in reality is with Attacker.

Detection and Prevention

1) Detection:-

SSL stripping can be identified in several ways. The most obvious way to see if your connection is made via SSL stripping is to look up the web address in the search bar. If SSL stripping occurs, http will be next to the web address, as opposed to http. Also, the lock at the left end of the search bar appears open or red, meaning the connection is not in the HTTPS format you want. Another way to find out if SSL stripping has taken place is to look for any incorrect design details on the website. If you suspect SSL stripping has taken place, finding small details on a webpage that look different from the legal ones can alert you. A slight change in the company logo, lack of multiple pages on the website or spelling errors will let you know that this website is not what you expected.

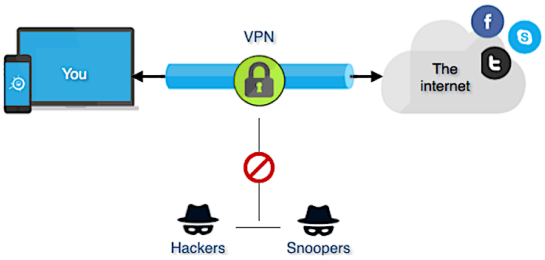
2) Prevention:-

One of the best ways to prevent SSL stripping is to look for inconsistencies in the search bar or webpage. Once you are alert about this threat, you may be looking for SSL stripping attacks frequently. Team members in your organization should also be aware of this threat to protect themselves and the organization from SSL stripping. Training classes by experienced team members or trained professionals go a long way in protecting sensitive data. Another way to protect web browsers from SSL stripping is to manually enter the URL in the search bar.

One of the biggest protections against SSL stripping is the use of HTTP strict transport security. HTTP Strict Transport Security or HSTS is a policy that only websites allow connections that use HTTPS connections. This prevents attackers from using SSL stripping to connect users to websites through an HTTP connection. Requests that use an HTTP connection are automatically redirected via HTTPS connection with HSTS. Once the HTTP Strict Transport Security comes into effect, your domain name will be added to the HSTS preload list. This list is used by many other search engines to block any HTTP connections from Google Chrome, Mozilla Firefox and other browsers.

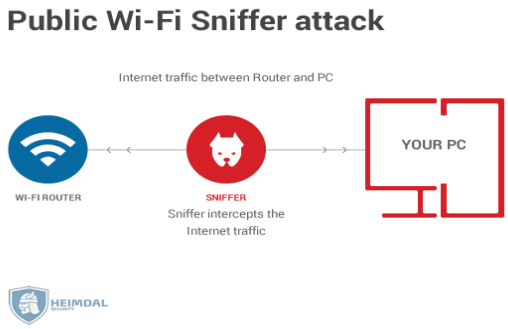
You can use some last steps in your environment to protect yourself from SSL stripping: -

Use of Virtual Private Networks: Virtual private networks or VPNs protect user data on websites regardless of connection type. If a user uses a VPN while viewing an HTTP website, the data will be encrypted due to the virtual private



network. This extra security layer helps the entire network or a single user.

Preventing Public Wi-Fi: Public Wi-Fi hotspots, especially airport Wi-Fi hotspots, are ideal for humans in Middle Attacks. Sensitive data can be easily intercepted or the user redirected to malicious websites via public Wi-Fi.



Cookies and Bookmarks: If you are on a trusted network, bookmark your websites where you enter sensitive information. Once you reach a website with HTTPS, such as a banking website, bookmark a secure website for future use, as the bookmarked website will always have an HTTPS connection. Additionally, enabling secure cookies ensures that all cookie data is provided with secure features.

Unknown links and HTTPS: The most obvious, but often occurring way to prevent SSL stripping is to never click on suspicious links and never accept connections to a website that does not have HTTPS. If a website has an HTTP connection, leave the website and retype the URL.

Practical Implementation

Even if SSL Strip or another similar program application is used, the first thing an attacker does is change the proxy between the browser and the web server. The software has the ability to encode modified URLs via SSL stripping, but it can intercept or forward data flow.

The following three methods are common in the implementation:

Incorrect entry of the proxy in the browser options: When targeting your system, the target is the browser more often than the entire computer. The malware ensures that the external proxy server automatically logs into the settings without the user knowing.

ARP or NDP Spoofing: In the subnet, attackers may revert to ARP spoofing (IPv4) or NDP-spoofing (IPv6) to run their proxy. The purpose of both protocols is to resolve IP addresses as corresponding hardware addresses (also known as MAC addresses). By using manipulated messages from these

protocols, the attacker can replace the requested hardware addresses with their own system addresses, and then intercept the transmitted data packets.

Providing your own hotspot: The third option is that the device running the server proxy also acts as a router. As a standard gateway, including the DHCP server, it can assign IP addresses to users and read and forward packets sent over subnet boundaries. This provides an accurate basis for SSL stripping.
After executing the proxy, the attacker does not have to do much for SSL strip: it runs a tool that sends altered links when needed. If successful, it will also send unencrypted information such as bank- or user-login data.

Conclusion

Hence by this paper we can conclude that SSL Stripping is serious threat used by attackers to steal confidential and sensitive data and there are many tools by which we can protect ourselves from this type of attacks such that use of HTTP strict transport security, Use of Virtual Private Networks, Preventing Public Wi-Fi, Unknown links and HTTPS.

References

1. https://www.https.in/ssl-security
2. https://www.eurodns.com/blog/ssl-stripping-attack-prevention
3. https://doubleoctopus.com/security-wiki/threats-and-tools/ssl-stripping/