Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study of Cookies and Threats to Cookies

Rajinder Singh
Research Scholar
DCSA PUSSGRC, Hoshiarpur,
Punjab, India

Dr. Satish Kumar
Ph.D. Supervisor
DCSA PUSSGRC, Hoshiarpur,
Punjab, India

Abstract—one of the main threats to network is session hijacking which can be carried out with the help of cookie exploitation. An HTTP cookie is a small piece of data or text file which is sent from a website or server and it is stored in the client side web browser while the user is browsing it. Cookies are created when a user visits a website and that website uses cookies to keep track the movements of the user. Main threats which are related to cookies are a) Sniffing network traffic for cookies b) XSS attack c) Cross-site request forgery (CSRF) Attack d) Session Fixation Attack. By using any of these methods an attacker can find out the cookie and can use it to carry out session hijacking.

Keywords: Cookie; XSS; CSRF; Session Fixation;

I. INTRODUCTION

Wireless networks have become very popular and important nowadays. Main advantages of wireless networks are that provide mobility and flexibility to the users or clients. Today's computer networks are vulnerable to various types of attacks. One of the main threats to network is **session hijacking** which can be carried out with the help of cookie exploitation. An HTTP cookie is a small piece of data or text file which is sent from a website or server and it is stored in the client side web browser while the user is browsing it. Cookies are created when a user visits a website and that website uses cookies to keep track the movements of the user. Every time user visits the web site, browser sends the cookie value to the server to notify the previous activity of the user to server. Cookies are plain text and do not contain any executable code. Cookies are used to store the various activities of the users on a website such as clicking particular buttons, logging in, or recording pages history of a web site. Server instructs client side browser to store this cookie information and then send its value back with each request. With this information server is able to identify the individual users [1] [2].

Mainly cookie store following information: name of the cookie, value of cookie, expiration date of the cookie, and valid domain name of the cookie, valid cookie path, and security information for the cookie.

II. TYPES OF COOKIES

Different types of cookies which are used to maintain the state of a web site are given below:

a). Session cookie:

It is also called a transient cookie and it contains information about a user. It is deleted when the user close the web browser. It is stored in temporary memory of the user's computer.

b). Persistent cookie:

Persistent cookies is not deleted when the user close the web browser. It is deleted at a particular date or after a particular time. With the help of this cookie web server remembers user's setting and information when user visit that web site later. Main information stored in this cookie is authentication information, language, menu preferences and bookmarks or favourites of visiting site [3].

c). Secure cookie:

These cookies are encrypted when they are transferred.

d). HttpOnly cookie:

HttpOnly cookies can only be used when transmitted via HTTP protocol or by HTTPS protocol. It is stored in user's hard drive. Main advantage of using this cookie is that they cannot be steeled through XSS vulnerabilities.

e).Third-party cookie:

Third party cookies are those cookies which are written on a client by a web site that is not actually visited by the user. These types of cookies are created by a webpage that loads the content from another web page. Main use of using such kind of cookies is tracking the behaviour of the users. Then they share this information to the advertising companies[4].

f). Supercookie

It is a type of browser cookie that is permanently stored on a user's computer. These are used for tracking technologies that do not rely on HTTP cookies. Main difference between regular cookie and super cookie is that they cannot be deleted in similar manner as regular cookie. Super cookies also do the same function as regular cookies. They are used to store information like browsing history, authentication data and ad related data [5].

g). Zombie cookie

These cookies are automatically recreated after being deleted by a client side script [1].

III. MAIN USES OF COOKIES

1) A cookie stores the current state of a web page of a website in the user's computer. This information helps users navigate between the pages of website efficiently.
2) With the help of cookie a web server can also identify the number of visitors visiting the site.
3) Cookies can also store user preferences and settings so that the user visits the site again then same preferences can be loaded again by the web server.
4) Cookies can also used to track the time user spends on the website.
5) Cookies also allow users to customize website to their interest [6].

Structure of Cookie:

Main components of cookie are Name and Values [7]. Other attributes of the cookies are [8]

a) Secure:

Cookie can be stolen by sniffing. So to overcome this problem cookie data is encrypted before it sends across the network. Encrypting cookie data means if in case an attacker sniffs data he/she will not be able to read data, thus ensuring safety of cookie data. But still nowadays many applications encrypt only login page of web site and only other sensitive page of web site. Other request for the data such as image files or small clip files are sent without the server without using encryption. But cookies are also sent across the network with these requests, and an attacker is still able to sniff the data and can steal session information from these cookies. Moreover some sites allow both type of communication using HTTP as well as HTTPS. So in these cases it is important to send cookie only over HTTPS connections and not at HTTP. And this is done with the help of secure attribute of a cookie.

b) Domain:

This attributes determines domain for which this cookie is valid or not.

Path: This attributes determines the path or URL for which the cookie is valid. The default path for this attribute is '/'.

Both the above said attributes are used to determine the scope of the cookie.

c) HTTPOnly:

Value of this attribute is used to check whether the client-side scripts are allowed to access the cookie or not.

d) Expires

This attribute is used to determine the time and date when the browser will delete the cookie.

Picture given below shows the various attributes of cookie.

Figure 1 Various Attributes of Cookie

IV. WORKING OF COOKIES

When a user types a url in the web browser then the browser sends a request to the web server. Now when web server receives a request from the browser, it first looks for the cookies. If cookie is not there then it creates a cookie with a unique id for the given request and then passes it to the user. The cookie is stored on the user's hard disk. Then various settings as well as preferences are also stored in the website database with a link to the cookie. Now if the user visits the same site again then cookie is also forwarded and web server from the stored database pulls the same preferences and gives to user.

V. MAIN THREATS RELATED TO COOKIES ARE

1) Sniffing Network Traffic for Cookies:

Main softwares which can be used to sniff the cookies are listed below:

- wireshark ,
- kismet,

- microsoft network monitor
- cain and able
- CommView

Earlier all the websites were using http protocol and not https protocol. So at that time Main packet analyzer which was used to sniff the cookies was wireshark. It is still used for sniffing purposes. Still there are web sites which are not able to use https in proper ways. So wireshark can be used to sniff the cookies [9].
Pictures given below demonstrate cookie sniffed by wireshark and chrome extension.

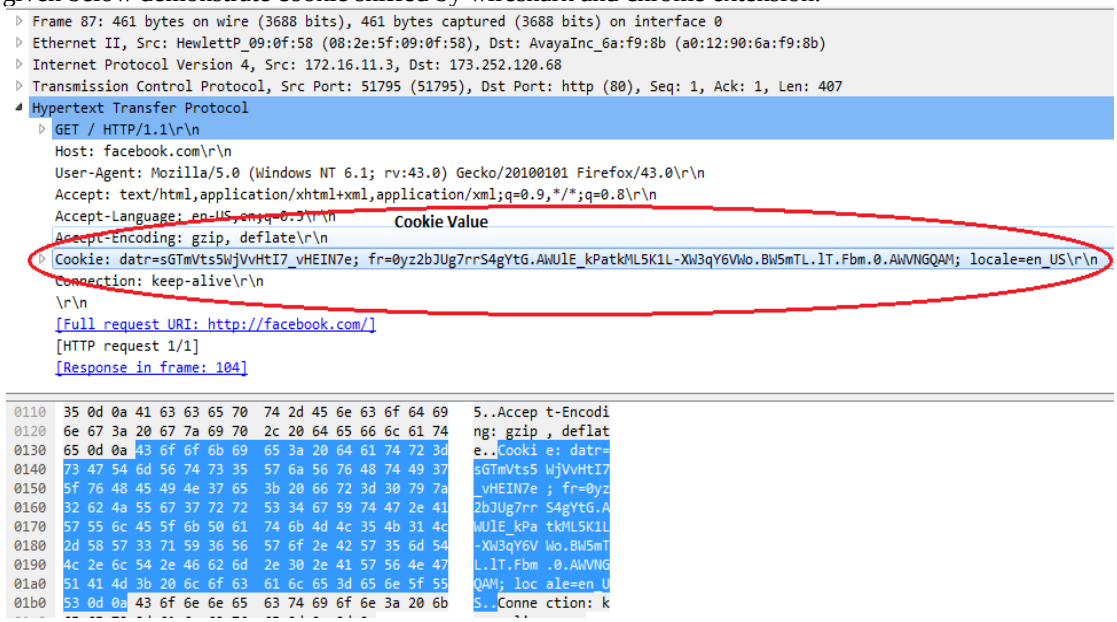

Figure 2 Finding Cookie by Wireshark

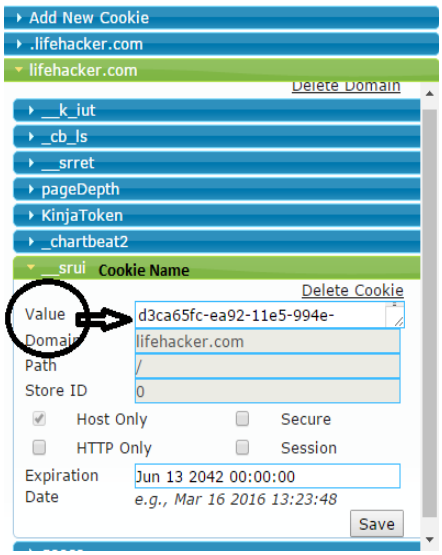

Figure 2 Cookie value by Chrome Extension

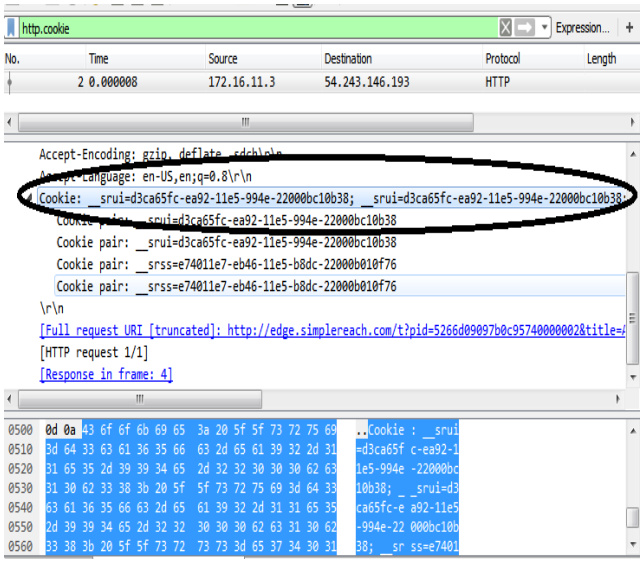

Figure 3 Cooke value by Wireshark

Remedy:
Some methods to avoid sniffing of cookies are given below:
1. Encrypting data. Try to use SSL/HTTPS encryption for the entire web site.
2. Using a long number or string instead of small number or string as the session key. So an attacker is not able to brute force the session-id.
3. Changing browser settings for restricting cookies.
4. Clearing the history and cookies from the browser. It can be done with the help of browser or from third party software like CCleaner [10].

2) Cross-Site Scripting Attack
This method is also very common for stealing the cookies. In this type of attack an attacker steals cookie information by making user clicking on a link that contains a malicious script. This script code reads cookie information and sends this information to the attacker by mail [11].

There are three types of XSS.
a) Stored XSS b) Reflected XSS c) DOM-based XSS.

a) Stored XSS:

In this case an attacker stores the malicious code permanently on the target servers e.g. in a database, log file or in a comment field etc. The victim when navigate the affected web page then he receives the malicious code from the server. It means that victims will end-up executing the malicious code once the page is opened in the browser.
The malicious code can be in JavaScript, HTML, and Flash or in any other type of code that the browser can execute it [12] [13].

b) Reflected XSS:

In a reflected XSS attack, the attacker's malicious code is a part of the victim's request which is sent to web server. The website then sends this malicious code to the victim as a response. The victim's browser executes this malicious script and sends cookies to the attacker's server [14].

c) DOM-based XSS

DOM-based XSS is a client side attack. DOM means document object model and it is used by HTML for working with the objects. When a script is executed client-side browser, it provides the code with the DOM of the HTML page in order to access various properties and values of that page. In this case attacker injects the malicious code as part of DOM and it is executed when the data is read back from the DOM.

Remedy:

Some methods for removing XSS attacks are:
1. Filtering means passing external data through a filter which will remove the dangerous keywords.
2. Escaping means by escaping dangerous character with the help of escaping characters [15] [16].

3) Cross-site request forgery (CSRF) Attack

In this type of attack an attacker forces a logged in user to perform an important action without his consent or knowledge. This attack can also be used to modify firewall settings, posting unauthorized data or even to conduct fraudulent financial transactions [17] [18].

Remedy:

Some methods which are used or proposed for preventing CSRF attacks are given below:
1) Using a Synchronizer token pattern
Main Characteristics of a CSRF Token are
   a) It should be Unique for per user & per user session
   b) It should have large random value
   c) It should be generated by a cryptographically secure algorithm
2) By checking the referer header
3) By Checking The Origin Header
4) By using Challenge-Response technique such as CAPTCHA or Re-Authentication (password) [19] [20].

4) Session Fixation Attack

Session fixation attacks exploit the vulnerability of a system which allows one person to find another person's session identifier.

Remedy:

Some methods which are used or proposed for preventing Session Fixation attack are given below:
1) Main defense is coding web applications correctly
2) Regenerating a new session identifier (SID) for each request [21] [22] [23].

VI. CONCLUSIONS

There are many web sites which are vulnerable to cookie theft. In this paper various methods which are used by the attacker to steal the cookies are discussed. Possible prevention measures for safeguarding the cookies are also discussed.

REFERENCES

[1] https://en.wikipedia.org/wiki/HTTP_cookie#cite_note-1
[2] https://www.nczonline.net/blog/2009/05/05/http-cookies-explained/
[3] http://www.allaboutcookies.org/cookies/persistent-cookies-used-for.html
[4] http://cookiecontroller.com/internet-cookies/third-party-cookies/
[5] https://www.techopedia.com/definition/27310/super-cookie
[6] http://resources.infosecinstitute.com/risk-associated-cookies/
[7] https://en.wikipedia.org/wiki/HTTP_cookie
[8] http://www.paladion.net/cookie-attributes-and-their-importance/
[9] https://en.wikipedia.org/wiki/Packet_analyzer
[10] https://en.wikipedia.org/wiki/Session_hijacking

[11] http://www.paladion.net/cross-site-scripting-attacks/
[12] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
[13] http://www.acunetix.com/websitesecurity/xss/
[14] http://excess-xss.com/
[15] http://www.acunetix.com/blog/articles/preventing-xss-attacks/
[16] http://resources.infosecinstitute.com/how-to-prevent-cross-site-scripting-attacks/
[17] https://www.tinfoilsecurity.com/blog/what-is-cross-site-request-forgery-csrf
[18] http://searchsoftwarequality.techtarget.com/definition/cross-site-request-forgery
[19] https://en.wikipedia.org/wiki/Cross-site_request_forgery
[20] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
[21] http://www.computerweekly.com/answer/Session-fixation-protection-How-to-stop-session-fixation-attacks
[22] https://en.wikipedia.org/wiki/Session_fixation
[23] https://coffeeonthekeyboard.com/best-basic-security-practices-especially-with-django-697/

