# OPTIMAL LINEAR CYBER – ATTACK ON WEB APPLICATION AND MITM ATTACK

P.Priya [#1] and P. Sivakamasundari [*2]

[#] *M.E - II Year,Dept of CSE, Adhiparasakthi Engineering College, Melmaruvathur.India*
[*] *Assistant Professor/CSE, Adhiparasakthi Engineering College, Melmaruvathur.India*

***Abstract*— The iRate Intelligent Decision Engine is a URL or Domain scanner which gives rating (Bad or Safe to visit) for a given domain. Basically it works like a MAV engine (Multiple Anti-Virus), but here it gets the ratings from various top security domains that provide the rating of the given domain. Added to this, it checks whether the domain or URL given is present in any of the domain blacklist sites. It also provides I Category- the category classification for the given domain. So this gives the analyst an advantage of having the Domain rating for the given domain with a lookup on top blacklist providing sites and also the Category Classification for the given domain. The effective detector exploits the intrusive component created by the adversary, followed by a secure beam forming-assisted data transmission. In addition to the solid detection performance, this scheme is also capable of obtaining the estimations of both legitimate and illegitimate channels, which allows the users to achieve secure communication in the presence of MITM attack**

***Index Terms*—Cber Attack, Web application, MITM attack**

## I. INTRODUCTION

The iRate Intelligent Decision Engine is a URL or Domain scanner which gives rating (Bad or Safe to visit) for a given domain. Basically it works like a MAV engine (Multiple Anti-Virus), but here it gets the ratings from various top security domains that provide the rating of the given domain. The IP spoofing attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The IP spoofing attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

### A. *SESSION SNIFFING*

In the example, as we can see, first the attacker uses a sniffer to capture a valid token session called "Session ID", then he uses the valid token session to gain unauthorized access to the Web Server.

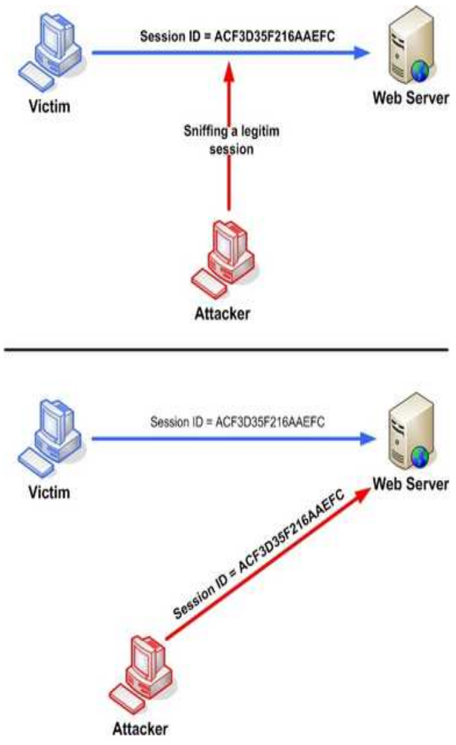

Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Figure1.1: Manipulating the token session executing the IP spoofing attack.

Cyber Security, the most talked about topic and the most concerned area in today's online world. The numerous numbers of complaints were received about hacking acts. People around there, using internet medium for most of their sort of stuff including business, communication, fun have a fear of being observed or hacked by malicious users. IP spoofing is achieved because of many reasons like insecure handling, no provision of account Lockout for invalid session IDs, indefinite expiration time as well as weak session ID generation code. IP spoofing refers to exploit a valid computer session where an hacker takes over a session between two systems. Tan intention besides stealing valid session ID is to get into system and steal the desired data.

## II. EXISTING SYSTEM

When examining a suspicious file, it is often useful to scan it with multiple antivirus tools. Sometimes one AV product might identify the file as malware, while another might not. The main drawbacks Multiple engines simultaneously can result in conflicts that lead to system freezes and application failures. In that virus database is not updated automatically .The upload file and download file size is limited.

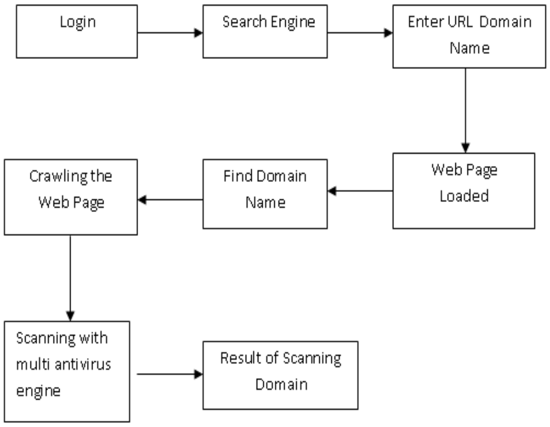
## III. PROPOSED SYSTEM

To prevent advanced threats that might be missed by anti-malware engines from entering your organization, it can sanitize potentially dangerous file types to thwart zero-day and targeted attacks. In addition, to identify and block files that have spoofed file type extensions, which indicates potential malicious of scanning data with anti-malware engines first, leveraging the power of their individual heuristic analyses, followed by converting potentially risky files to remove embedded threats greatly decreases the chances of your network being infected by an unknown threat. For MITM our Packets can encrypted with SHA-1 algorithm and its generated with the random key, Packets are modify by authorised system only if hackers try to modified it will be rejected automatically. The advantages of this project Multiple engines are scan one by one it's not affect the system like freezes. The virus definitions are updated automatically. It each and every domains present in that link.

## IV. SYSTEM ARCHITECTURE

The architecture involves the URL or domain scanner which gives rating for a given domain using iRate search engine. It gets the ratings from various top security domain that provides the rating of the given domain. The detector exploits the intrusive component created by the adversary, followed by a secure beam forming – assisted data transmission. The users to achieve secure communication in the presence of MITM attack.

### A. IRate Search Engine



### B. IP Spoofing

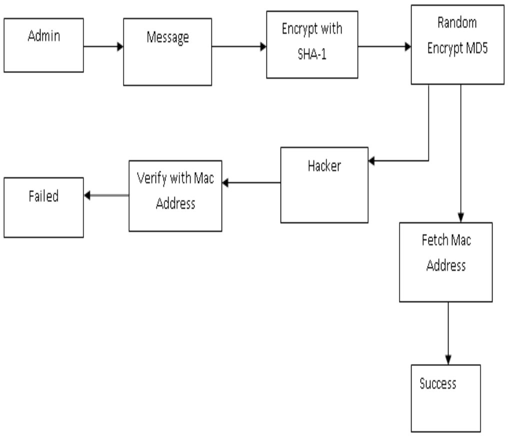


Figure 1.2 Architecture diagram

## V. SYSTEM MODULES

### A. BLUECOAT WEB CATEGORY

The Blue Coat WebFilter database contains Web site ratings representing billions of Web pages, published in more than 50 languages, and organized into useful categories to enable customers to better monitor, control, and secure their Web traffic. Blue Coat WebFilter is supported by Blue Coat's powerful WebPulse cloud community.

### B. FIREGUARD WEB CATEGORY

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

### C. TREND URL SAFETY RATING

Scores are assigned based on factors such as a website's age, historical locations, changes, and indications of suspicious activities discovered through malware behavior analysis. We've advanced how we apply web reputation to keep pace with new types of criminal attacks that can come and go very quickly, or try to stay hidden.

### D. COOKIE MANAGEMENT

The attacker uses packet sniffing to read network traffic between two parties to steal the session cookie. Many web sites use SSL encryption for login pages to prevent attackers from seeing the password, but do not use encryption for the rest of the site once authenticated. This allows attackers that can read the network traffic to intercept all the data that is submitted to the server or web pages viewed by the client. Since this data includes the session cookie, it allows him to impersonate the victim, even if the password itself is not compromised. Unsecured Wi-Fi hotspots are particularly vulnerable, as anyone sharing the network will generally be able to read most of the web traffic between other nodes and the access point.

### *E. MAGIC COOKIE*

A magic cookie, or just cookie for short, is a token or short packet of data passed between communicating programs, where the data is typically not meaningful to the recipient program. The contents are opaque and not usually interpreted until the recipient passes the cookie data back to the sender or perhaps another program at a later time. The cookie is often used like a ticket – to identify a particular event or transaction

### *F. IDLE TIMEOUT*

The other type of session attack is session fixation. Here, instead of stealing/hijacking the victim's session, the attacker fixes the user's session ID before the user even logs into the target server (that is, before authentication), thereby eliminating the need to obtain the user's session ID afterwards. Before going into detail of session fixation attacks, we must classify two types of sessions managed on Web servers:

Permissive sessions allow the client's browser to propose any session ID, and create a new session with that ID if one does not exist. After that, the server continues to authenticate the client with the given ID.

Strict sessions allow only server-side-generated session ID values.

A successful session fixation attack is generally carried out in three phases:

Phase I or session set-up: In this phase, the attackers set up a legitimate session with the Web application, and obtain their session ID. However, in some cases the established trap session needs to be maintained (kept alive) by repeatedly sending requests referencing it, to avoid idle session time-out.

Phase II or fixation phase: Here, attackers need to introduce their session ID to the victim's browser, thereby fixing the session.

Phase III or entrance phase: Finally, the attacker waits until the victim logs into the Web server, using the previous session ID.

## VI. CONCLUSION

iRate and MAV engine technique provides the rating of the given domain and the details of the blacklist sites along with its category classification.

IP spoofing application here provides awareness in users about their security due to insecure handling weak session IDs and mostly no account lockout. In order to prevent this,one must apply the countermeasures in their daily routine of internet access.

## REFERENCES

[1] Internet Crime Complaint Centre link: www.ic3.gov

[2] Liu, Bingchang; Shi, Liang; Cai, Zhuhua; Li, Min; "Software vunerability Discovery Techniques : A Survey" IEEE Conference Publication, DOI : 10.1109/MINES.2012.202, Page(s) 152-156, 2012 .

[3] Smith, Yurick, Doss "Ethical Hacking" IEEE Conference Publication, DOI: 10.1147/sj.403.0769, Page(s): 769-780

[4] Bradley, Rubin "Computer Security Education and Research: Handle with care" IEEE Conference Publication, DOI : 10.1109/MSP.2006.146, Page(s): 56-59

[5] Wilbanks "When Black Hats are really white" IEEE Conference Publication, DOI: 10.1109/MITP.2008.146, Page(s): 64

[6] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack tothe HTTPS protocol," IEEE Security and Privacy Magazine, no. 1, pp.78–81, 2009.