© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

ENHANCEMENT OF HTTP SERVER SECURITY TO PREVENT ATTACKS ON COMMERCIAL

[1]Sunil , Research Scholar,Department of CSE, Indus Instt. of Engg. & Tech, jind.
[2]Abhishek bhatnagar, A.P., Department of CSE, Indus Instt. of Engg. & Tech, jind

ABSTRACT: HTTP is an application layer protocol designed within framework of Internet Protocol Suite. Its definition presumes an underlying & reliable transport layer protocol,[2] & Transmission Control Protocol is commonly used. However HTTP could be adapted to use unreliable protocols such as User Datagram Protocol, for example within HTTPU & Simple Service Discovery Protocol. There are several threat to HTTP server security. Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant with within order to attack from full range of threat agents, from hackers to nation-states. System must be capable to restrict damage & recovery from occurrence of attacks. The objective of research is to secure HTTP server from external attacks.

ISSN : 2278-6848
03
9 772278 684800
© International Journal for Research Publication and Seminar

[1] Introduction

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is foundation of data communication for World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is protocol to exchange or transfer hypertext. Development of HTTP was initiated by Tim Berners-Lee at CERN within 1989. Standards development of HTTP was coordinated by Internet Engineering Task Force (IETF) & World Wide Web Consortium (W3C), culminating within publication of a series of Requests for Comments (RFCs). The first definition of HTTP/1.1, version of HTTP within common use, occurred within RFC 2068 within 1997, although this was obsoleted by RFC 2616 within 1999.

A later version, successor HTTP/2, was standardized within 2015, then supported by major web browsers & already supported by major web servers. HTTP functions as a request–response protocol within client–server computing model. A web browser, for example, may be *client* & an application running on a computer hosting a web site may be *server*. The client submits an HTTP *request* message to server. The server, which provides *resources* such as HTML files & other content, or performs other functions on behalf of client, returns a *response* message to client. The response contains completion status information about request & may also contain requested content within its message body. Web browser is an example of a *user agent*. Other types of user agent consists of indexing software used by search providers voice browsers, mobile apps, & other software that accesses, consumes, or displays web content.HTTP is designed to permit intermediate network elements to improve or enable communications between clients & servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

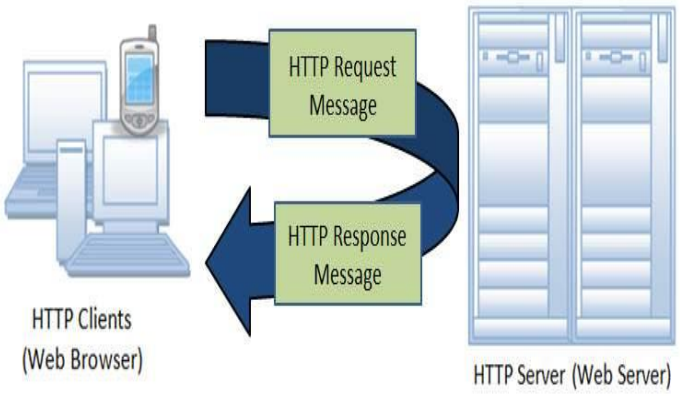


Fig 1 The **Hypertext Transfer Protocol**

HTTP resources are identified & located on network by uniform resource locators (URLs), using uniform resource identifier (URI) schemes *http* & *https*. URIs & hyperlinks within Hypertext Markup Language (HTML) documents form inter-linked hypertext documents.

HTTP/1.1 is a revision of original HTTP (HTTP/1.0). In HTTP/1.0 a separate connection to same server is made for every resource request. HTTP/1.1 could reuse a connection multiple times to download images, scripts, stylesheets, *etc* after page has been delivered. HTTP/1.1 communications therefore experience less latency as establishment of TCP connections presents considerable overhead.

[2] Literature Review

Butler W. Lampson wrote on "Computer Security within Real World"

In a distributed system with no central management like Internet, security requires a clear story about who is trusted for each step within establishing it, & why. The basic tool for telling this story is "speaks for" relation between principals that describes how authority is delegated, that is, who trusts whom. The idea is simple, & this explains what's going on within any system I know. The many different ways of encoding this relation often make this hard to see underlying order.

Hailu Tegenaw (2015) within his research paper **"Application Aware Firewall Architecture to Enhance Performance of Enterprise Network (978-1-4799-7498-6/15©2015 IEEE)" stated that** performance of an enterprise network is affected not only by its protocol specification, its communication channel, design capacity & architecture of firewall but also by its implementation & traffic management. It was considered that Firewall is a perimeter security solution that is useful for addressing network traffic. It introduces a single point through which all traffic passes & as a result this creates performance bottleneck on enterprise network by increasing latency, reducing bandwidth & throughput.

Sangita A. Jaju(2015) within this research paper **"A Modified RSA Algorithm to Enhance Security for Digital Signature (978-1-4799-6908-1/15©2015 IEEE)"** stated that digital signature has been providing security services tosecure electronic transaction over internet. Rivest, Shamir & Adlemen (RSA) algorithm was most widely used to provide security technique. Here they have modified RSA algorithm to enhance its level of security. This paper presents a fair comparison between RSA & Modified RSA algorithm along with time & security by running several encryption & decryption setting to process dataof different sizes. The efficiency of these algorithms was considered based on key generation speed & security level. The texts of different sizes were encrypted & decrypted using RSA & modified RSA algorithms. The simulation result proves that within Modified RSA algorithm key generation is faster & this enhances security by two levels. RSA algorithm is faster than Modified RSA within terms of encryption & decryption speed.

Ayman Tajeddine, Ayman Kayssi, Ali Chehab, Imad Elhajj (Department of Electrical & Computer Engineering) (2014) presented a paper **"Authentication Schemes for Wireless Sensor Networks" within 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014.**

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

In this paper, they discussed different authentication techniques suitable for severely constrained nodes within wireless sensor networks. They divide such techniques into three main categories based on symmetric cryptography, asymmetric cryptography, & hybrid techniques using both cryptographic methods. They discussed each category & deduce best cipher for each, namely, RC5 & IBE-ECC to be applied within a WSN. They also specify factors affecting decision of which category is best to use & different parameters affecting network within each category. Finally, they give a real network example & discuss appropriate choice of authentication scheme based on particular WSN needs.

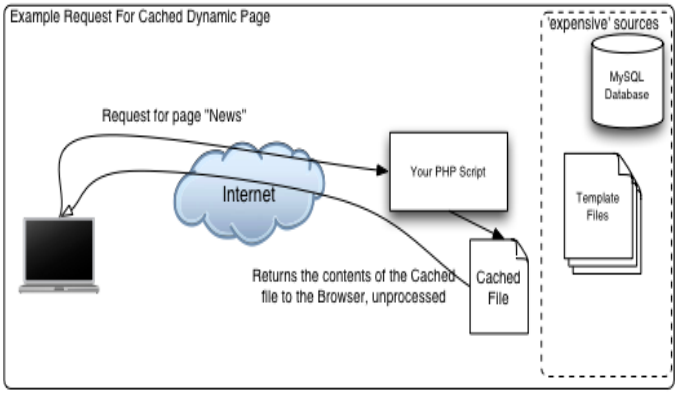
[3] RESEARCH METHODOLOGIES

HTTP session

An HTTP session is a sequence of network request-response transactions. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80, occasionally port 8080; see List of TCP & UDP port numbers). An HTTP server listening on that port waits for a client's request message. Upon receiving request, server sends back a status line, such as "HTTP/1.1 200 OK", & a message of its own. The body of this message is typically requested resource, although an error message or other information may also be returned.

HTTP Authentication

HTTP provides multiple authentication schemes such as Basic access authentication & Digest access authentication which operate via a challenge-response mechanism whereby server identifies & issues a challenge before serving requested content.



.fig 2 HTTP server

Authentication Realms

The HTTP Authentication spec also provides an arbitrary, implementation specific construct for further dividing resources common to a given root URI. The realm value string, if present, is combined with canonical root URI to form protection space component of challenge. This within effect allows server to define separate authentication scopes under one root URI

[4] PROBLEM FORMULATION

Security

The TRACE method could be used as part of a class of attacks known as cross-site tracing; for that reason, common security advice is for this to be disabled within server configuration. Microsoft IIS supports a proprietary "TRACK" method, which behaves similarly, & which is likewise recommended to be disabled.

HTTP Method	RFC	Request Has Body	Response Has Body	Safe	Idempotent	Cacheable
GET	RFC 7231	No	Yes	Yes	Yes	Yes
HEAD	RFC 7231	No	No	Yes	Yes	Yes

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

HTTP Method	RFC	Request Has Body	Response Has Body	Safe	Idempotent	Cacheable
POST	RFC 7231	Yes	Yes	No	No	Yes
PUT	RFC 7231	Yes	Yes	No	Yes	No
DELETE	RFC 7231	No	Yes	No	Yes	No
CONNECT	RFC 7231	Yes	Yes	No	No	No
OPTIONS	RFC 7231	No	Yes	Yes	Yes	No
TRACE	RFC 7231	No	Yes	Yes	Yes	No
PATCH	RFC 5789	Yes	Yes	No	No	Yes

Table 1 Status codes

[5] Implementation

WebBrowser	Secure browsing kb/s	Insecure Browsing kb/s
Firefox	20	23
Internet Explorer	19	22
Google Chrome	22	25

Table 2 Secure web browsing/Insecure browsing

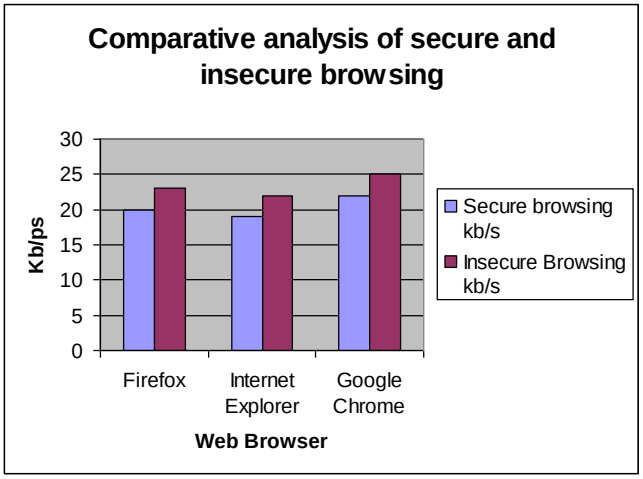


Fig 3 Comparative Analysis of secure and insecure browsing

Web page count	Time Taken(IE)	Time Taken(Firefox)	Time Taken(chrome)
1	3	2	2
2	4	3	2
3	5	3	3
4	6	6	4
5	8	8	6
5	8	7	6
6	9	9	7
7	10	9	8
8	10	10	9
10	12	11	10
11	12	12	11
12	14	13	13
13	14	14	14
14	16	15	15
15	16	16	15

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

Table 3 Table for insecure browsing in case of different web pages

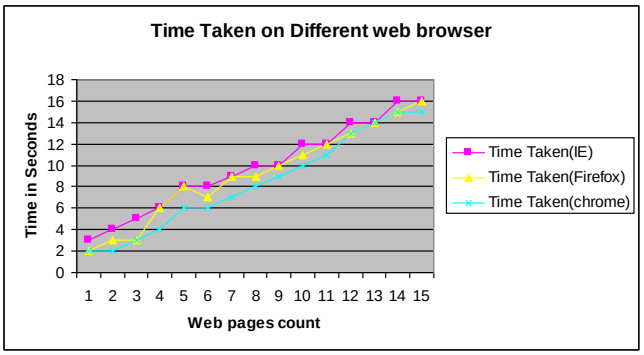


Fig 4 Chart for insecure browsing in case of different web pages

Web page count	Time Taken (IE)	Time Taken (Firefox)	Time Taken (chrome)
1	4	3	2
2	5	4	4
3	6	5	4
4	7	6	6
5	9	8	7
5	9	8	8
6	10	10	9
7	11	10	10
8	11	11	10
10	13	12	11
11	13	13	12
12	15	15	14
13	16	15	15
14	17	16	16
15	18	17	17

Table 4 Table for secure browsing in case of different web pages

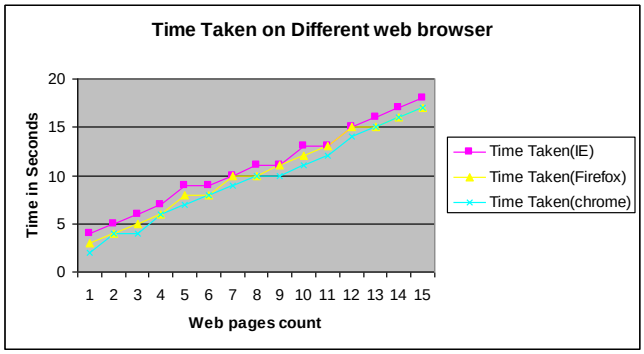


Fig 5 Chart for secure browsing in case of different web pages

[6] CONCLUSION

Security of HTTP server is must as there are several E-commerce websites where buy & selling of goods take place. So security of HTTP Server is must from Hacking.

Hacking has both its benefits & risks. Hackers are very diverse. They might bankrupt company or might protect data, increasing revenues for company. Battle btw ethical or white hat hackers & black hat hacker has been long war, that has no end. While ethical hacker help to understand companies' their security needs, malicious hackers intrudes illegally & harm network for their personal benefits. Ethical & creative hacking has been significant within network security, within order to ensure that company's data has been well protected & secure. At same time this allows company to identify, & within turn, to take remedial measures to rectify loopholes that exists within security system, that might allow malicious hacker to breach their security system. They help organizations to understand present hidden problems within their servers & corporate network. Study also reveals that valid users are ethical hackers, till their intensions are clear otherwise they are great threat, as they have access to every piece of data of organization, as compare to total & semi outsiders. This also concludes that hacking has been important aspect of computer world. This deals with both sides of being good &

bad. Ethical hacking plays vital role within maintaining & saving lot of secret data, whereas malicious hacking could destroy everything. What all depends has been intension of hacker. This has been almost impossible to fill gap btw ethical & malicious hacking as human mind cannot be conquered, but security measures could be tighten.

Reference:

1. Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (June 1999). Hypertext Transfer Protocol -- HTTP/1.1. IETF. RFC 2616. "Overall Operation". p. 12. sec. 1.4. RFC 2616.

2. Berners-Lee, Tim. "HyperText Transfer Protocol". World Wide Web Consortium. Retrieved 31 August 2010.

3. Tim Berners-Lee. "The Original HTTP as defined within 1991". World Wide Web Consortium. Retrieved 24 July 2010.

4. Raggett, Dave. "Dave Raggett's Bio". World Wide Web Consortium. Retrieved 11 June 2010.

5. Raggett, Dave; Berners-Lee, Tim. "Hypertext Transfer Protocol Working Group". World Wide Web Consortium. Retrieved 29 September 2010.

6. Raggett, Dave. "HTTP WG Plans". World Wide Web Consortium. Retrieved 29 September 2010.

7. Simon Spero. "Progress on HTTP-NG". World Wide Web Consortium. Retrieved 11 June 2010.

8. "HTTP/1.1". Webcom.com Glossary entry. Retrieved 2009-05-29.

9. Fielding, Roy T.; Reschke, Julian F. (June 2014). Hypertext Transfer Protocol (HTTP/1.1): Authentication. IETF. RFC 7235.

10. Berners-Lee, Tim; Fielding, Roy T.; Nielsen, Henrik Frystyk. "Method Definitions".

11. Hypertext Transfer Protocol -- HTTP/1.0. IETF. pp. 30-32. sec. 8. RFC 1945. "Method Definitions". pp. 51-57. sec. 9. RFC 2616.

12. Jacobs, Ian (2004). "URIs, Addressability, & use of HTTP GET & POST". Technical Architecture Group finding. W3C. Retrieved 26 September 2010.