A PROXY-BASED ADAPTIVE SECURITY MODEL FOR SECURE SOCKET LAYER (SSL) ECOSYSTEM

[1]Suhairi Mohd Jawi, [2]Fakariah Hani Mohd Ali, [3]Nurul Huda Nik Zulkipli

[1,2,3] *Faculty of Computer and Mathematical Sciences, UiTM Shah Alam, Selangor, Malaysia*

[1]suhairi@cybersecurity.my,[2]fakariah@tmsk.uitm.edu.my, [3]nhuda@tmsk.uitm.edu.my

Abstract

Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) has been the main drivers for secure communication over the web. Since its first inception, these protocols face with several security issues from their design and implementation. Several solutions and proposals have emerged as measures to enhance their security. The study for adaptive security for SSL/TLS deserves a focus. In this study, components from adaptive security such as monitoring, analysis and response are integrated into a web proxy. One of the advantages of adaptive security is its architecture improves over time. It can help in protecting users from security threats of HTTPS connections in the changing security environments.

Keywords*: Secure Socket Layer;* Transport Layer Security*; adaptive; proxy*

1. Introduction

SSL/TLS used in Hypertext Transfer Protocol Secure (HTTPS) is used to create a secure communication channel for the web and other connections such as for electronic mail and file transfer. However, SSL/TLS implementations have encountered many security issues such as weak protocol implementation, bad SSL certificates and man-in-the-middle (MITM) attacks.

This research will use adaptive security model to tackle some of the issues. The model is implemented as a web proxy that processes HTTPS connection from web clients such as web browsers. A web based management system will be developed to provide controls to the proxy.

2. Previous and Current Solutions

There are several solutions have been proposed and developed by academia as well as industry in improving the state of SSL protocol.

Multiple-Channel SSL (MC-SSL) which was proposed by Song *et al*. (2004) does not use adaptive methods but provides multiple-channel for SSL session via application proxies or gateways but server or / and client are to trust the proxy unconditionally.

Meanwhile, Lamprecht *et al*. (2007) proposed Adaptive SSL (ASSL) renegotiation within SSL session on the server side implemented as a module for Apache web server. Renegotiation can be activated as the environment changes. The factors can be the threat level, server load, transaction type, or client attributes such as processing power, bandwidth or type of client.

For the industry, CA/Browser Forum introduces Extended Validation Certificate (EV) SSL which uses domain-validated certificates for authentication of the domain name (Larry,

2009). Meanwhile, security researcher Moxie Marlinspike developed *Convergence* as a beta project based on ideas from Carnegie Mellon University (Mathew, 2011). It works as an add-on for Firefox browser to replace the functionality of existing CA infrastructure. In addition, The Tor Project and the Electronic Frontier Foundation (EFF) had developed a Firefox extension called as HTTPS-Everywhere that rewrites web traffic for some major websites that mix their contents between HTTP and HTTPS.

3. Adaptive Security Models

There are several models had been proposed to implement adaptive security for a security system inclusive of its design, components and behaviours. Basically, the idea is to interconnect the components into a set of intercommunicating objects. The purpose of each component varies in term of the objectives for the specific system. However, each model usually has the following components (Marcus, 2004):

1) Monitoring component,
2) Analysis component, and
3) Response component

Besides these three components, another pivotal role is the components connectivity. This connectivity relies on some manifestation between these components. To manifest the events to the expected results, many models rely on security policy that works adaptively for each model.

Followings are the models that had been developed including a survey by a research paper Elkhodary *et al*. (2004) to show how software system might adapt its security mechanisms at runtime.

1) Complex Information System (CIS) (Shnitko, 2004)
2) Adaptive Security Infrastructure (ASI) (Marcus, 2004)
3) Extensible Security Infrastructure (ESI) (Elkhodary *et al*., 2007)
4) The Willow Architecture (Elkhodary *et al*., 2007)
5) Adaptive Trust Negotiation and Access Control (ATNAC) (Ryutov *et al*., 2005)

Table 1 summarizes the above models in order to understand their monitoring, analysis and respond components.

Table 1: Comparison of different adaptive security models

Models	Monitoring	Analysis	Response	Component Connectivity
Complex Information System (CIS)	Detector Device (DD)	Analyzer Device (AD)	Responder Device (RD)	Control Objects (CO)
Adaptive Security Infrastructure (ASI)	Detector	Analyzer and Policy Engine	Responder	Pervasive Hierarchy Assumption (PHA)
Extensible Security Infrastructure (ESI)	Events	Conditions	Respond	Written into a policy file
The Willow Architecture	Control Loops	Reactive Controller	Infrastructure Self Defense	Sets of finite state machines
Adaptive Trust	TrustBuilder	Analyzer (a	GAA-API	Extended Access

Negotiation and Access Control (ATNAC)		GAA-API module)		Control List (EACL)

4. Proxy-Based Adaptive Model for SSL/TLS

The design for adaptive security proxy for SSL/TLS will follow closely the adaptive security models above. For the proxy, its implementation will contain:

A. Security Policy

Security policy shall be developed first to create a security baseline for a system to isolate and eliminate threats.

B. Monitoring component

This captures all environment variables from client browsers and certificate information from SSL-enabled web server to be used for analysis.

C. Analysis component

This will do some analysis based on security policy and application logs described later in the proposed design. It also contains inline processing for server certificates using OpenSSL.

D. Response component

This component is responsible for allowing or denying connection to SSL-enabled web server based on the analysis done on particular sites.

5. Methods

The model uses a forward proxy with adaptive security features for SSL/TLS connections as in Figure 1. Common method for SSL proxy-ing is called SSL tunneling or HTTP CONNECT method as specified by some Internet-Drafts [1]. However, CONNECT method is a purely pass-through connection. The proxy only transparently redirects the data between client and server. It only knows the source and destination addresses; and does not interfere with the transaction. Therefore, CONNECT method that employs blind passing of SSL/TLS transaction can be enhanced to include adaptive security features to solve SSL/TLS problems.

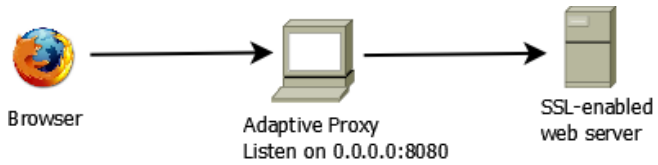

Figure 1: Placement of adaptive proxy for SSL/TLS connection.

In brief, the solution proposed here are as in Figure 2:

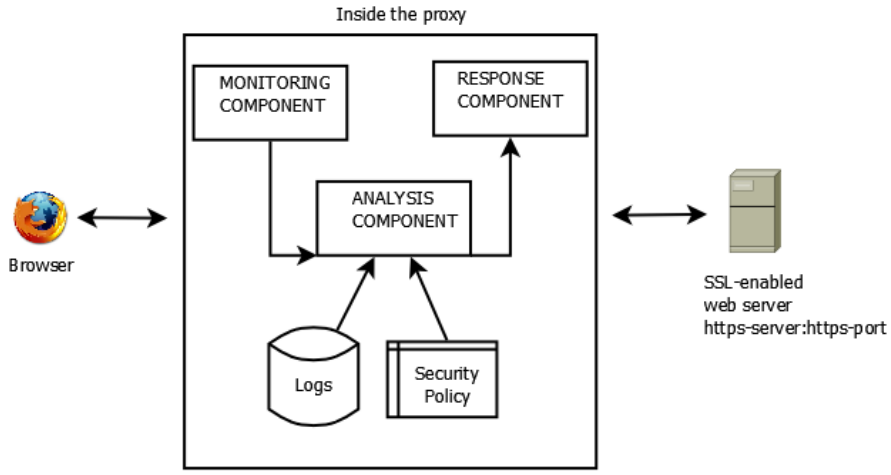

Figure 2: Adaptive proxy components.

A. Security Policy

Security policy shall be developed first for insertion into analysis component. Policy definition will be based on Extended Access Control List (EACL) as used by GAA-API (Ryutov et al., 2005). EACL evaluates its statements using Backus-Naur Form (BNF) to give positive and negative access rights. A parser that can interpret BNF will be developed in order to parse the policy.

B. Monitoring Component

Figure 3 shows the monitoring component inside the proxy that monitors HTTPS requests and response back and forth between a client and a SSL-enabled web server. CONNECT method is primarily of interest for this research to establish end-to-end tunnel connection to the target server via a proxy.

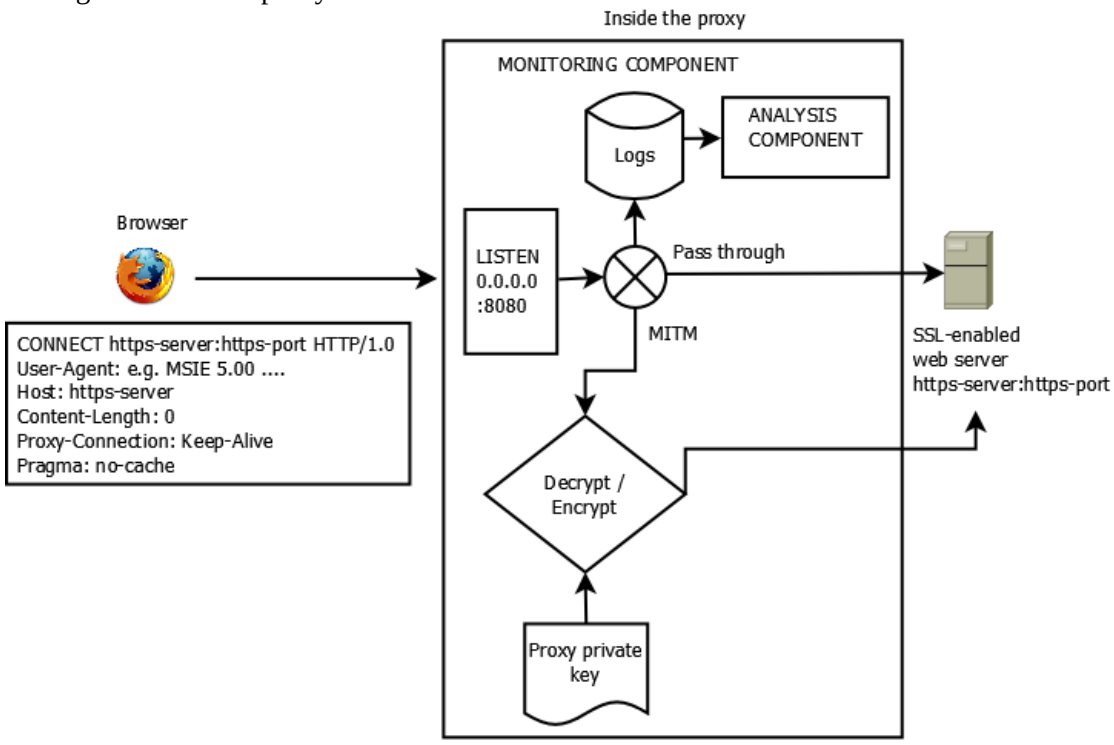

Figure 3: Monitoring component inside the proxy.

The proxy can be operated in dual mode based on the level of current security threat defined by proxy administrator following the security policy. Analysis component will be run concurrently but may not be in real-time. However, once the analysis is already finished, the subsequent requests to the same web server may get security alerts from the proxy's response component if the analysis components find any security threats regarding SSL/TLS connection.

a. Pass through mode

   When the security threat is low, a pass through mode will be deployed. The analysis part is still working as usual but only limited to analysis of server certificate and current URLs being requested.

b. MITM mode

   In the event of threat level being escalated to high or severe, then the MITM mode will be used. Request from client browser and response from server will be decrypted and re-encrypt for analysis of malicious contents such as malware payload and phishing websites.

C. Analysis Component

This is the second component of the adaptive proxy as shown in Figure 4. It consists of security policy and analyzer for SSL certificates, HTTPS capabilities of the web server and its raw contents. It takes input from Monitoring component that stored in log file and does some filtering or pattern matching action according to rules defined in security policy.

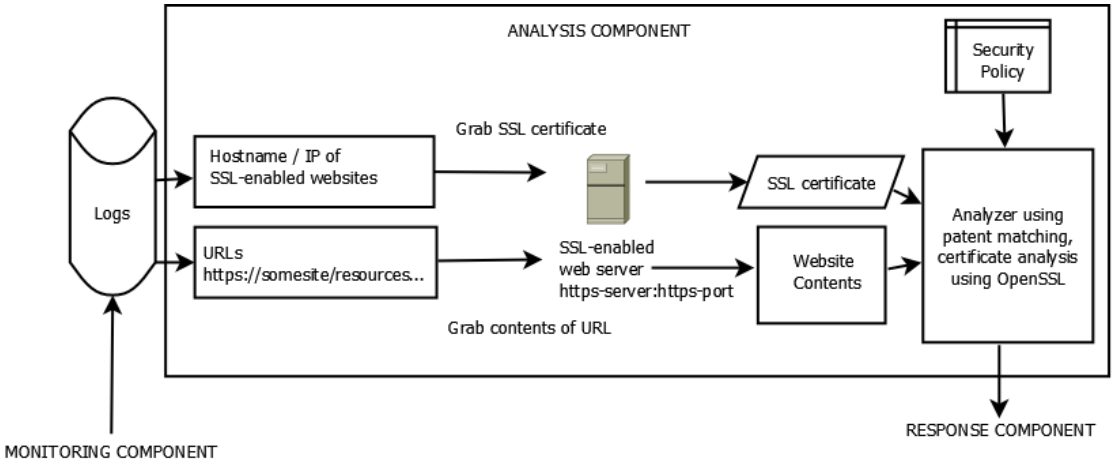

Figure 4: Analysis component inside the proxy.

This analysis will much concern with the replies the proxy received from intended server in the form of server certificates and HTML source from URL. In order to obtain the server certificate, the following OpenSSL command will be used.

```
$ openssl s_client -connect mail.google.com:443
```

Meanwhile, grabbing URL contents can be done using Unix tools such as *curl* or *wget*.

```
$ wget https://mail.google.com
$ curl https://mail.google.com
```

Running external commands above requires proxy to handle the execution care. Proxy may not wait the execution to finish. It can spawn the process as a new program asynchronously. Otherwise, the proxy may become hanged while waiting for the command to finish.

D. Response Component

Response is the output of the analysis once criteria in the rule are matched as shown in the Figure 5. It can allow a connection, renegotiate SSL session or terminate it. For logging purposes, every action may need to give a reason especially for session termination.

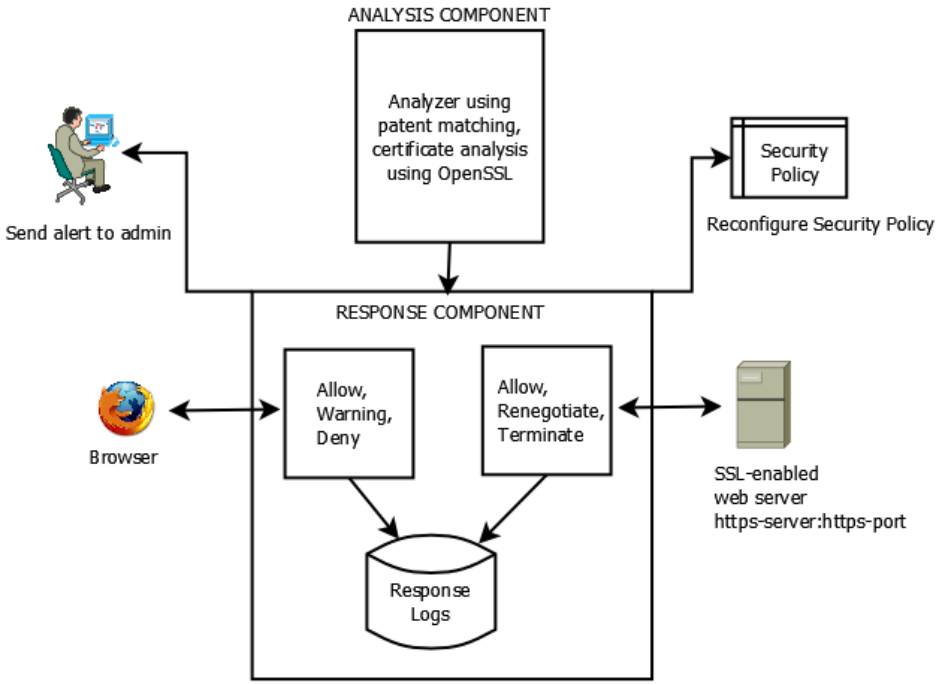

Figure 5: Response component inside the proxy.

Response component consists of several outputs as follows:

a. Message to users

Proxy will issue appropriate message to clients in the form of HTML pop-up or inline message while browsing on secure sites using the proxy as the connection gateway. This eliminates the need to have browser add-on to conveying the state of SSL/TLS connection. Clients will be notified if the site being visited is using valid certificates inclusive of some certificate information such as certificate issuer, validity period and company information.

b. Alert to administrator

Any security threat detected by the proxy shall be alerted to administrator.

c. Security policy reconfiguration

Response shall suggest policy reconfiguration in order to strengthen the analysis done by the proxy.

E. Proxy Administration

Proxy will be run as a daemon (background process) which can be started or shutdown from a command line. Proxy will listen on port 8080 which is greater than 1024 (ephemeral port). If port number is less than 1024, then proxy may get port binding errors.

For adaptive components, a web based interface for configuration, maintenance of rule sets, viewing reports and logs will be developed. It comes with forms to change the proxy settings, modify the rules and to start or stop the proxy. Reports and logs will be shown in tabular format and graphs / charts for ease of understanding and analysis.

6. Conclusions

SSL protocol is a suitable choice for secure transaction over the web but it counters many security issues. The proposed solution can be further studied for adaptivity in handling the threats and risks over SSL protocol. The response from this model can be either in the change of cipher suite likes Adaptive SSL does or just alerting the users about the health of their SSL session. In the worst case scenario, blocking users from reaching the affected sites can be the last alternative for security but require appropriate message notified to them.

References

Y. Song, V.C.M. Leung and K. Beznosov, *Supporting endto-end security across proxies with multiple-channel SSL,* in Proc. IFIP SEC, Tolouse, France, Aug. 2004

C. J. Lamprecht and A. P. A. van Moorsel. *Adaptive SSL: Design, Implementation and Overhead Analysis*, First International Conference on Self-Adaptive and Self-Organizing Systems, 2007. SASO '07., pp. 289-294, 2007.

Larry Seltzer, *Spoofing Server-Server Communication: How You Can Prevent It*, 2009

Mathew J. Schwart, *New SSL Alternative: Support Grows for Convergence*, InformationWeek, 30th Sept 2011

L. Marcus, *Introduction to Logical Foundations of an Adaptive Security Infrastructure paper and slide presentation*, Proc. of the Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), A sub-workshop of the LICS Foundations of Computer Security (FCS'04) Workshop, LICS '04,

A. Shnitko, *Pratical and theoretical issues on adaptive security*, in Proceedings of FCS'04 Workshop on Foundations of Computer Security, ser. General Publications, A. Sabelfeld, Ed., vol. ISBN:952-12-1372-8, no. 31, June 2004, pp. 267–282.

A. Elkhodary and J. Whittle, *A survey of approaches to adaptive application security*, SEAMS '07, May 20-26,2007.

T. Ryutov, L. Zhou, C. Neuman, T. Leithead, K. Seamons, *Adaptive Trust Negotiation and Access Control*, ACM Symposium on Access Control Models and Technologies, pps. 139-146, 2005