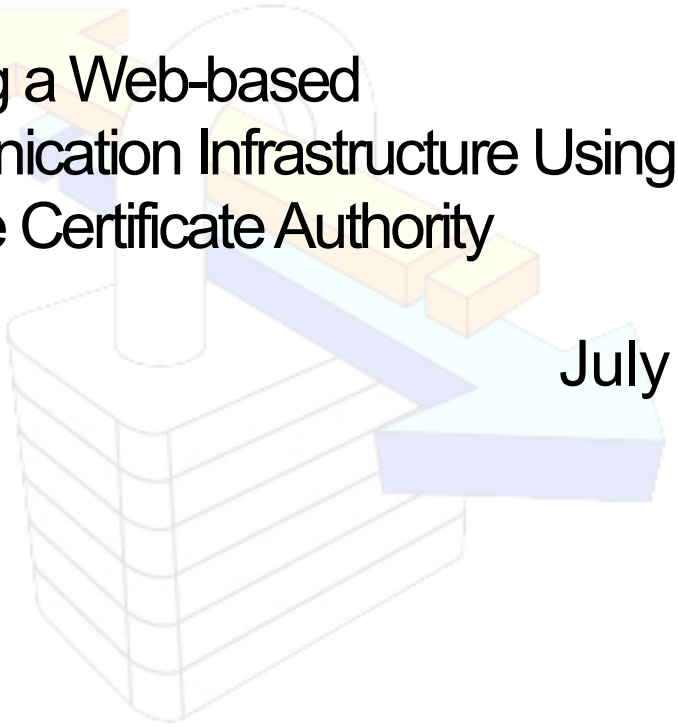
A Technical White Paper from Waubonsie Consulting

Apache and OpenSSL

Securing a Web-based Communication Infrastructure Using a Private Certificate Authority

July 2002



Waubonsie Consulting

Waubonsie Consulting
The Apache Integration Experts
<http://www.waubonsie.com>
<info@waubonsie.com>

Waubonsie Consulting

Apache and OpenSSL: Securing a Web-based Communication Infrastructure Using a Private Certificate Authority.

Table of Contents

Introduction

Today's web-based communication channels allow corporations and organizations greater flexibility in transacting mission critical data as never before. With this new found flexibility corporations and organizations are facing a disconcerting problem: How to retain the great flexibility of data sharing using the World Wide Web without compromising the valuable data being shared.

The following technical paper discusses how two open source tools, the popular Apache Web Server and the OpenSSL PKI Toolkit can secure a web-based communication infrastructure such that the flexibility of the World Wide Web can be used to share valuable business data while at the same time limiting the risk of disclosing the information being shared to unauthorized parties.

ESO Plastics' Communication Problem

A would-be plastic manufacturing corporation named ESO Plastics needs to communicate valuable information between its employees, vendors and customers in its aggressive industry, in a flexible manner to give the company an advantage in bringing new products to market. This communication method needs to be secure such that the valuable data in transit is not compromised or leaked to a rival consumer plastics company by eavesdropping or false identification. In addition, this communication method needs to limit the risk of corporate information from being accessible by former employees or venders should the company experience a period of high turnover.

One method for ESO Plastics to pursue is to develop an in-house application for its employees and vendors to use when communicating with ESO Plastics. This traditional desktop modem application can then dial a dedicated phone number to transfer information to ESO Plastics using an internally developed method for authentication and encryption. While implementing this infrastructure would allow ESO Plastics' employees and vendors the flexibility to communicate with ESO Plastics from just about any location, it would require a year to develop the proper client/server applications along with integrating the applications with ESO Plastics' databases. However, the cost in personnel alone could top $200,000, just for the first year of development[1]. This communication framework would also require maintaining a telecommunications network dedicated solely for client's application to connect to. Additionally, it would require another communication method, such as a corporate website running an e-commerce application, for ESO Plastics' customers who are not in direct contact with ESO Plastics to use in purchasing of ESO's products. The time delay and expense are critical obstacles to solving their problem.

ESO Plastics' Communication Solution

Secure Socket Layer Protocol

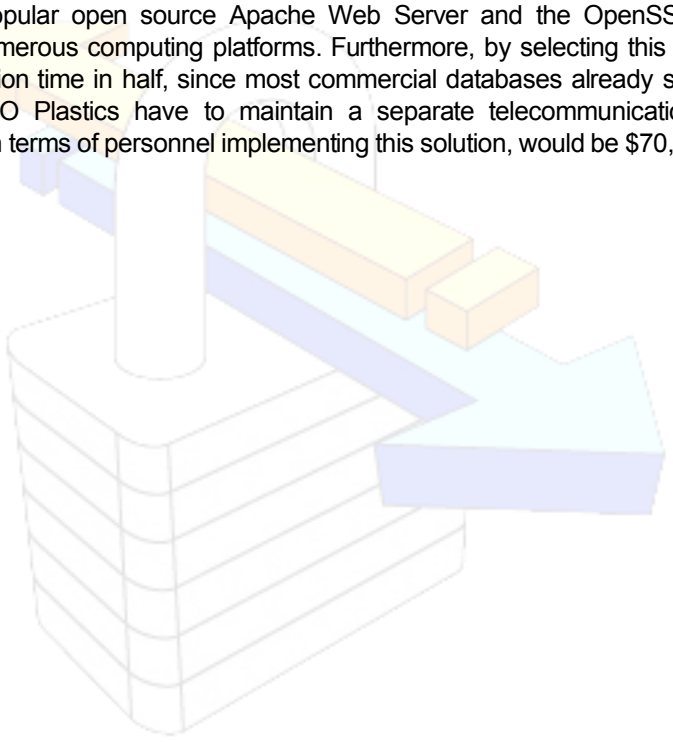
The Secure Socket Layer (SSL), developed by Netscape Communications[2], and Transport Layer Security (TLS), an open-standard replacement for SSL[3], add ciphers for encryption and digital certificates for authentication to the HTTP protocol, providing a method to translate various models of trust to the World Wide Web.

Apache and OpenSSL

The Apache Web Server, developed and maintained by The Apache Group and The OpenSSL PKI Toolkit, developed and maintained by The OpenSSL Project provide the software implementation of the main protocols, SSL, TLS and HTTP. The OpenSSL Toolkit also provides the main functionality for creating and maintaining a

Certificate Authority and the Digital Certificates created by the Certificate Authority. An Apache Module, mod_ssl, enables the functionality of the OpenSSL toolkit within the Apache Web Server. The Apache Module mod_ssl was developed and is maintained by Ralf Engelschall.

An alternative solution for ESO Plastics is to develop and implement a communication method using the standard HTTP protocol, allowing all three parties; employees, vendors and customers to communicate with ESO Plastics using a Web-based (HTTP) interface. ESO Plastics has also selected the standard SSL and TLS protocol as its method of providing encryption and authentication to secure the transaction of information over the World Wide Web. By selecting this communication framework ESO Plastics has bypassed the need to develop client/server applications since client web applications such as Microsoft's Internet Explorer or the open source Mozilla web browser along with server applications such as the popular open source Apache Web Server and the OpenSSL Toolkit are available, without fee, for numerous computing platforms. Furthermore, by selecting this method, ESO Plastics will cut their integration time in half, since most commercial databases already support HTTP, SSL and TLS. Nor will ESO Plastics have to maintain a separate telecommunications structure. Overall, ESO Plastics' cost, in terms of personnel implementing this solution, would be $70,000[4].



Encryption and Authentication

The Features of SSL and TLS Protocol

The two main functions of SSL and TLS are to enable the encryption of data between two parties and provide for the authentication of the two parties transacting the data[5].

Two different types of ciphers, Symmetric and Asymmetric are used within the SSL and TLS protocol.

Ciphers

> Symmetric ciphers, also known as secret-key ciphers, use a single key for both encrypting and decrypting data. In the case of Symmetric ciphers the encrypted data is secure only as long as the key used for encryption and decryption is kept secured.
>
> Asymmetric ciphers use a key pair, consisting of a public key and private key, to encrypt and decrypt data. The public key encrypts data only. The private key is used to decrypt the data. Therefore, data encoded with the public key is secure as long as the private key stays secure.

Used alone, both ciphers have their shortcomings. Symmetric encoded data can be considered secure only so long as the key used for encryption and decryption is kept secured. Asymmetric encoded data uses larger CPU usage for mathematical computation, thus reducing the overall performance of a computer's potential. SSL and TLS works around these limitations by using both types of ciphers. First an Asymmetric cipher is used to securely exchange a Symmetric key. Then using a Symmetric key the actual data is transferred between the two communicating parties, thus reducing CPU usage.

ESO Plastics has determined that their public website should include the functionality of allowing customers the ability to purchase pre-manufactured plastic molds from their online catalog. To facilitate a secure environment for transacting purchasing information online ESO Plastics has deployed an Apache-based commercial web server with the SSL and TLS functionality enabled.

The second feature of the SSL and TLS protocol is Digital Certificates.

Digital Certificates

> Digital Certificates supply distinguishing information, such as a corporation's operating information or an employee's name, as a method of authentication[6].

Public Certificate Authorities, like Verisign[7], Thawte[8] or Equifax[9], are corporations that act as a trusted third party validating distinguishing information that is used by the communication parties for authentication.

In regards to ESO Plastics' public website, ESO Plastics has requested and installed a digital certificate from Verisign that provides the distinguishing information about ESO Plastics and their website. A customer using ESO Plastics' online catalog to purchase a pre-manufactured plastic molding can use the distinguishing information provided by Verisign's digital certificate to verify that the web server that is transacting the encrypted purchasing information with the customer's web browser does indeed belong to ESO Plastics.

The Private Certificate Authority

The Internal Communication Framework

Intranet

> An Intranet is an in-house website, which may link to the Internet, serving as a reference point for an organization and is not accessible to the general public. Web-based applications can be built on Intranets, providing capability to multiple computer platforms such as Macintosh, Windows and Linux[10].

ESO Plastics has implemented an Intranet using Apache and mod_ssl to create a secure interface method to a web-based application for its employees. The web-based application allows the employees from various offices to manage their employment records with a centralized Human Resources department. Within this system employees can provide personal information, such as providing direct deposit account information for paychecks, in a secure online environment.

Private Certificate Authority

> A Private Certificate Authority, similar to a Public Certificate Authority, acts as a trusted party validating identifying information about the communicating parties for authentication. Private Certificate Authorities are used when some kind of trust relationship already exists, such as between an employee and the employer[11].

ESO Plastics, acting as a private certificate authority, is using its relationship to its employees a model of trust. For example, it has validated that the domain name *intranet.esoplastics.com* is indeed its own Intranet server. The Intranet server will pass the digital certificate, to whoever establishes a connection to it. Since employees already have an established relationship with ESO Plastics to base their trust on, when connecting to the server and receiving the digital certificate signed by ESO Plastic's certificate authority they can trust that the information identifying *intranet.esoplastics.com* as ESO Plastic's Intranet site is validated. Thus, the employee can be assured that the personal information the employee is sending is encrypted to *intranet.esoplastics.com*, and it is indeed going to ESO Plastic's web application for the Human Resources department.

Of course, ESO Plastics will want to authenticate access to the Intranet for employees only. Also, it wants to ensure that only the proper employee can access and submit information about them. ESO Plastics has configured their Apache server to require clients to present digital certificates signed by ESO Plastics to gain access to the Intranet server since other methods, such as login/passwords pairs, are less secure. Moreover, the web-based application is configured to access Apache's Environment Variables to provide further validation by comparing the distinguishing information about the employee, such as their name or corporate email address from the digital certificate, with the employee's information as already stored in the application's database.

Root Certificate

> A Digital Certificate that identifies a Certificate Authority.

Each employee's web browser at ESO Plastics, as well as ESO Plastics' Intranet server, has the root certificate that identifies ESO Plastics' certificate authority installed allowing for proper identification of digital certificates signed by ESO Plastics' certificate authority.

Extranet

> An Extranet is a website designed for a specific audience, such as for business customers rather than the general public. Usually it provides access to specific information such as research, current inventories, or internal databases; virtually any information that is private and not published for everyone. An Extranet uses the public Internet as its transmission system, but requires user authentication for entrance. Access to the site may be free or require payment for some or all of the services offered[12].

For example, ESO Plastics has a relationship with a number of vendors that supply it with raw materials and equipment. ESO Plastics has established a continuing relationship with Moldings Holdings, Inc. where, Moldings Holdings develops molding equipment for ESO Plastics to use for the creation of various durable plastic products ESO Plastics sells. Part of this relationship requires employees for ESO Plastics to supply Moldings Holdings with specifications and requirements for development of new molding equipment.

Certificate Signing Request

> A Certificate Signing Request (CSR) is an encoded file with identifying information from one of the communicating parties, along with a public key sent to a certificate authority for validation. After validating the distinguishing information, the certificate authority digitally signs the encoded file creating a Digital Certificate.

To allow ESO Plastics employees access to the project development documents, Moldings Holdings has set up a secure area on their Extranet network. To authenticate the Extranet server for ESO Plastics' employees ESO Plastics has processed a certificate signing request from Moldings Holdings using OpenSSL, creating a digital certificate that Moldings Holdings can use. Once the digital certificate is created it will only be valid for a specified time frame, usually one year and can only be used on the server containing the private key matching public key encoded within the digital certificate, in this case, *eso.moldhold.com*.

As with ESO Plastics' Intranet, Moldings Holdings has configured its server to require digital certificates, signed by and identifying ESO Plastics' employees, before granting access to Molding Holdings' Extranet.

Since each ESO Plastics employee requests a digital certificate from the ESO Plastics' certificate authority, and before signing each request with OpenSSL the employment information is validated internally with Human Resources, all Moldings Holdings has to do is install a copy of the root certificate in its web server for identification of ESO Plastics' digital certificates. Moreover, Molding Holdings can use the department information that ESO Plastics requires in each employee digital certificate to limit access to Moldings Holdings' Extranet to only those ESO Plastic employees who are working on the development of molding equipment with Molding Holdings.

The main function of a certificate authority is to validate identifying information that will be used for authentication. Therefore, the first goal for a private certificate authority is to develop a method for not only confirming information at the time a digital certificate is requested, but also that the information is valid for the lifetime of the digital certificate itself.

Another example of how a private certificate authority is used can be seen in ESO Plastics' customer relationship with Van Stan Automotives. ESO Plastics is the exclusive supplier of plastic molds for Van Stan Automotives' dent resistant car doors. As with ESO Plastics' relationship with its vendor, Moldings Holdings, ESO Plastics has set up an Extranet and has installed their root certificate to validate incoming digital certificates. ESO Plastics has signed and installed a digital certificate for their Extranet server and they have signed a digital certificate request from Bob Smith, Van Stan Automotives' manager of Dent-be-Gone doors.

Certificate Revocation List

> A Certificate Revocation List (CRL) is a list of client certificates that were revoked before they expired. Clients with revoked client certificates will be denied access to a Client Authentication Realm if the revoked client certificates are in the server's CRL[13].

However, Bob Smith left Van Stan Automotives to work for another automotive corporation located in his hometown. Bob Smith's digital certificate doesn't expire until a few months after he plans to leave Van Stan Automotive. To ensure that Bob Smith doesn't try to access ESO Plastics' Extranet using the digital certificate he has installed on his personal laptop, thereby compromising Van Stan Automotives' valuable product information, as well as ESO Plastics' own customer relationship with Van Stan Automotive, ESO Plastics, acting in its role as certificate authority has revoked the digital certificate it issued to Bob Smith. After revoking the digital certificate, ESO Plastics creates a certificate revocation list that contains the unique serial number identifying Bob Smith's digital certificate. Once ESO Plastics' Extranet server is configured to read the certificate revocation list, the Apache-based server will verify that the incoming digital certificate being supplied by a client does not match the digital certificate that has been revoked by ESO Plastics' certificate authority and which is therefore no longer to trusted[14].

Conclusion

By setting up and running an Apache Web Server with OpenSSL, an organization or corporation can establish a secure environment that brings the flexibility of transacting information over the web within reach. The security of transacting information over the web using SSL and TLS allows a customer purchasing goods online to know that:

- The communication with the store is secure, so that no one can collect the customer's information while the data is in transit.
- The server on the other end, decrypting the data is, in fact, the online store, and the customer information will be used to process the order.

Or an employee of a corporation accessing the corporate Intranet/Extranet from their home or office knows, that:

- The communication between with the company is secure, so that no one can collect the company information while it is in transit.
- The server on one end of decryption is the company server and the information is valid.
- The client on the other end of decryption is, in fact, an employee and that the information has not been compromised.

ESO Plastics' Communication Solution

By setting up and running Apache and Apache-based Web Servers ESO Plastics has developed and implemented a communication method using the standard HTTP protocol, allowing all employees, vendors, and customers to communicate with ESO Plastics using various secured Web-based interfaces. By using mod_ssl and OpenSSL Toolkit ESO Plastics has been able to also implement the standard SSL and TLS protocols as its method of providing encryption and authentication to secure the transaction of information over the World Wide Web.

Additionally, in implementing this communication framework, ESO Plastics has bypassed the need to develop traditional client/server applications since client web applications such as Microsoft's Internet Explorer or the open source Mozilla web browsers already are available for numerous computing platforms.

ESO Plastics has cut their integration time in half, since most commercial databases already support HTTP, SSL and TLS, as well. Nor will ESO Plastics have to maintain a separate telecommunications structure.

Overall, ESO Plastics' cost in terms of personnel cost has been reduced by over half. Better yet, since the protocol and software ESO Plastics has chosen are computing standards, ESO Plastics can outsource their solution to a consulting firm for routine maintenance or implementation if desired[15].

Footnotes

[1] Based on national average salary as listed at Monster.com, <http://salary.monster.com>. 1 experienced Client/Server Programmer - $61,127, 1 experienced Project Lead - $79,776 and 1 experienced Telecommunications Engineer - $55,031 equals $195,934.

[2] See: <http://www.netscape.com/eng/ssl3/>

[3] See: <http://www.ietf.org/rfc/rfc2246.txt>

[4] Based on national average salary as listed at Monster.com, <http://salary.monster.com>. 1 experienced Web Software Developer - $61,416 and 1 experienced Project Lead - $79,776, over six months equals $70,596

[5] From: Weinstein, Paul. "Web Security: Encryption & Authentication." Daemonnews (May 2001): 15 pars. <http://www.daemonnews.org/200105/ssl_apache.html>

[6] From: Hirsch, Frederick “Introducing SSL and Certificates using SSLeay Summer 1997” <http://www.ultranet.com/~fhirsch/Papers/wwwj/article.html>

[7] See: <http://www.verisign.com>

[8] See: <http://www.thawte.com>

[9] See: <http://www.equifax.com>

[10] From: “TechEncyclopedia.” TechWeb: The Business Technology Network (12 July 2002) <http://www.techweb.com/encyclopedia>

[11] From: Weinstein, Paul. "Web Security: Encryption & Authentication." Daemonnews (May 2001): 15 pars. <http://www.daemonnews.org/200105/ssl_apache.html>

[12] From: “TechEncyclopedia.” TechWeb: The Business Technology Network (12 July 2002) <http://www.techweb.com/encyclopedia>

[13] From: Leach, Mike and Tim Starr “Using Certificate Revocation Lists.” Apache Week (12 December 2000): 22 pars. <http://www.apacheweek.com/issues/00-12-22>

[14] From: Leach, Mike and Tim Starr “Using Certificate Revocation Lists.” Apache Week (12 December 2000): 22 pars. <http://www.apacheweek.com/issues/00-12-22>

[15] See: <http://www.waubonsie.com>

About Waubonsie Consulting

The name Waubonsie belonged to a Potawatomi Indian chief who lived during the 1800s. As settlers moved across the American landscape, Chief Waubonsie, whose name literally means “early dawn”, conferred with the settlers on the “lay of the land”.

Waubonsie Consulting continues in the spirit of Chief Waubonsie in collaborating with settlers new and old about the “lay of the land” in the wake of the early dawning digital world.

Paul Weinstein, Chief Consultant and Founder of Waubonsie Consulting, has been working at the forefront of the Apache world for a number of years and understands how the world's most popular web server can bring your online solution together. From a Public Ecommerce Site to a Private Corporate Intranet, he's done it all. In fact, the Open Source and Internet Developer communities have welcomed him in discussing his knowledge at industry leading conferences and technical publications. That is experience you can count on.