

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Interested in learning more?

Check out the list of upcoming events offering "Security Essentials: Network, Endpoint, and Cloud (Security 401)" at http://www.giac.org/registration/gsec

### What is Secure Outlook Web Access (SSL-OWA)? Cliff Rittel

September 13, 2000

### What is OWA?

Microsoft OWA for Exchange Server offers the ability to access secure e-mail, calendar, scheduling and collaboration applications using the Internet Explorer Web Browser. A server running Exchange 5.5 and Internet Information Server are required on the backend. The IIS server uses active server pages to handle the requests and interact with the central log on server for authenticity and the Exchange Information Store for access to a mailbox. Mailbox information can only be accessed while client/server on-line connectivity exists. This application is used primarily as a central server application service, which remote clients connect to over the public Internet. Due to the inherent insecurity of the Internet, security settings such as SSL need to be put in place.

### What is ASP and SSL?

ASP is an acronym for Application Server Provider and refers to an environment where clients access a central server over the Internet, and the core data resides on the server. The OWA connection fits the ASP model because all of the data is centrally hosted and decentralized clients are accessing the data. Typically, ASP

SSL is an acronym for Secure Sockets Layer which is a protocol developed by Netscape Communications to provide secure data transmissions over the Internet. SSL is a transport layer security technique that can be applied to HTTP and provide privacy between two communicating devices, as this paper will demonstrate the Windows client and the Exchange/IIS server. SSL provides mandatory authentication, encryption and data integrity. The protocol mandates data transmissions by a session key so that data transmissions cannot be altered or disclosed. A more in depth understanding of the SSL transaction will be established in the next sections.

### Setup of OWA

For my test, I used Windows clients (98/NT/2000) connected to dial up, cable modem and T1 connections over the Internet to illustrate the ASP functionality. Please note IE is required as OWA connectivity will not work with Netscape or any other Internet Browser. I used NAI's Gauntlet 5.5 firewall and built a proxy to handle the connection. On the LAN, I used a standard Intel server configuration running Windows2000 SP1, Exchange 5.5 SP3 and IIS 5. For SSL I used a server certificate issued by a publicly trusted root CA, Thawte, and installed it on the IIS server. I only required server side authentication, but to add an additional layer of authentication security one could require the client have a valid SSL certificate (see IIS SSL ENABLE SETUP). Below is a diagram of the network topology, screen shots of the log on transaction and further explanation of the SSL/OWA and network authentication transaction.

## Client/Server SSL - OWA Setup & Network Authentication



### SSL Transaction

In order for the SSL transaction to work both the client (IE) and the Server (IIS) must be SSL enabled. The transaction runs over TCP. (1) The security transaction begins when the client sends a request to the server for its digital certificate. Traditionally, this begins with typing https: in the URL locator. (2) The server sends its digital

certificate to the client. The client will check the digital certificate for accuracy in terms of issuance from a trusted root Certificate Authority, valid date on the certificate and common name of the certificate. If there are any problems the user has the option to view the certificate, continue or cancel the transaction. (3) If the client continues, then the client authenticates the server by decrypting the digital signature that is within the digital certificate. The client then generates a session key and encrypts it using the server's public key from the certificate sends it to the server. Once the server receives the session key it uses it to encrypt and decrypt the data tunnel. SSL uses message authentication to ensure tampering with data transferred between the client and server has not taken place.

Example (2)

| Security | Alert  |
|----------|--|
| ß        | Information you exchange with this site cannot be viewed or<br>changed by others. However, there is a problem with the site's<br>security certificate. |
|          | The security certificate is from a trusted certifying authority.   |
|          | The security certificate date is valid.  |
|          | The name on the security certificate does not match the name of the site.  |
|          | Do you want to proceed?  |
|          | Yes <u>No</u> View Certificate   |

### Logon Authentication

Once the SSL session is established between the client and server, the server requests from the client a user alias mailbox on the client. (4) Then the client is prompted for its network logon credentials, which it then authenticates with a Logon Server. (5) Once authenticated with a valid user account the Exchange server offers the client access to their mailbox resources.

OWA Log On Mailbox Alias Screen



```
Network Logon Server Screen (4)
```

| Enter Net  | work Passwo           | rd ?×                          |
|------------|-----------------------|--------------------------------|
| <b>?</b> > | Please type yo        | our user name and password.    |
| 2          | Site:                 | exchangewest                   |
|            | Realm                 | exchangewest                   |
|            | <u>U</u> ser Name     |                                |
|            | <u>P</u> assword      |                                |
|            | □ <u>S</u> ave this p | password in your password list |
|            |                       | OK Cancel                      |

### Mailbox Resource Screen (5)

| 🎒 Microsoft ( | Jutlook Web Access - Micro     | soft Internet Explorer  |   |
|---------------|--------------------------------|---|---|
| File Edit     | View Favorites Tools He        | łp  |   |
| dack ▼        | → ⊗ ⊉<br>Forward Stop Refresh  | ☆ Q · G · G · Air<br>Home Search Favorites History Mail   | Drint Edit  |
| 🛛 Address 🧧 ł | https://exchangewest/exchange/ | root.asp  |   |
| inbox         | ₽ 🦻 📑 🖻 🔗  <br>Inbox           | 📸 📮 🕜   👔 Messages  | •   |
| Calendar      | E<br>© Inbox<br>©Storage       | ✓     !     !     .     .       □     ≥     Zague       □     ≥     ADCS-Cliff Rittel   | <b>Subject</b><br>MS Office Viewe<br>External helpdes:    |
| Contacts      |                                | Image: Contraction of the second s | RE: New Surfcor.<br>Disabling Print L<br>FW: Liebert Unit |
| Find<br>Names |                                | Image: ADCS-Cliff Rittel       Image: ADCS-Cliff Rittel       Image: ADCS-Cliff Rittel  | RE: New Helpde:<br>RE: wireless LA1                       |

### IIS SSL Enable Setup

As noted previously, the test installation was on a Windows2000 SP1 platform with Exchange Server 5.5 SP3 and Internet Information Server 5. The following screen shots give a graphical presentation on how to set up SSL within IIS. The SSL connection has additional security options such as requiring the browser to establish 128 bit encryption or mandating client certificates.

Properties of IIS Web Server

| Exchangewest Properties   | ? ×  |
|---|--|
| Web Site         Operators         Performance         ISAPI Filters           Directory Security         HTTP Headers         Custom   | Home Directory Documents<br>Errors Server Extensions   |
| Anonymous access and authentication control<br>Enable anonymous access and edit the<br>authentication methods for this resource.  | <u>E</u> dit   |
| Anonymous access No user name/password required to access this resource. Account used for anonymous access: Edit  | 1<br>  |
| Authenticated access<br>For the following authentication methods, user name and password are  |  |
| required when <ul> <li>anonymous access is disabled, or</li> <li>access is restricted using NTFS access control lists</li> </ul> Sector authentication (password is sent in clear text) | <u>S</u> erver Certificate<br><u>V</u> iew Certificate |
| Select a default domain: Edit  Digest authentication for Windows domain servers   | E <u>d</u> it  |
| Integrated Windows authentication      OK Cancel Help   | Apply Help   |
| UK Lancel Help  |  |

# Manage Secure Communications

| 🚡 Console1 - [Console Roo  | t]  |                                 | - <b>- ×</b> |
|--|---|---------------------------------|--------------|
| ] 🚡 <u>C</u> onsole <u>W</u> indow <u>H</u> e  | lp  | ] 🗋 (                           | 🎽 🖬 🔳 🎫      |
| <u>Action View Eavorites</u>   |   | ß                               |              |
| Tree Favorites   |   | ne<br>nternet Information Servi | ces          |
| Exchangewest<br>Scripts<br>Scripts<br>Scripts<br>IISHelp<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>IISAdmin<br>Scripts<br>Scripts<br>IISAdmin<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts<br>Scripts | Explore<br>Open<br>Browse<br>Start<br>Stop<br>Pause |                                 |              |
| ⊡ 🤯 Administration<br>⊕ 🍇 Default SMTP V   | New All Tasks New Window from Here                  |                                 |              |
| sheet for the c  | Delete<br>Refresh                                   |                                 |              |
|  | Properties  |                                 |              |
|  | Help  |                                 |              |

Very important security warning message

| Secure Communications  | х |
|--|---|
| Require secure channel (SSL)   |   |
| Require <u>1</u> 28-bit encryption   |   |
| Client certificates  |   |
| Ignore client certificates   |   |
| C Accept client certificates   |   |
| C Require client certificates  |   |
| Client certificates can be mapped to Windows user<br>accounts. This allows access control to resources<br>using client certificates. |   |
| Current CTL:   |   |
| Ne <u>w</u> Edjt   |   |
| OK Cancel <u>H</u> elp   |   |

This screen shows SSL connection options.

| Internet Service Manager 🛛 🗙   |
|--|
| The authentication option you have selected results in<br>passwords being transmitted over the network without data<br>encryption. Someone attempting to compromise your system<br>security could use a protocol analyzer to examine user<br>passwords during the authentication process. For more<br>detail on user authentication, consult the online help. This<br>warning does not apply to HTTPS(or SSL) connections. |
| Are you sure you want to continue?   |
| Yes <u>No</u> Help   |

### Conclusion

OWA over a SSL connection can offer an effective, secure communication over the public Internet to an Exchange mailbox. OWA operates as an ASP host, which increases the ability to tighten security in a central location. OWA installations without SSL are a security risk as users will send their passwords in clear text over the Internet. SSL ensures authentication, encryption and data integrity. When establishing any type of remote access into an internal network a well thought out plan is essential to ensure the highest level of security possible in protecting precious Information Systems.

### References

Microsoft Corporation. (1999). "Planning and Deploying Outlook Web Access 5.5". Microsoft Corporation. Redmond, WA. White Paper.

Microsoft Corporation (1999). "ASP Certification White Paper". Microsoft Corporation. Redmond, WA. http://www.microsoft.com/ISN/downloads/ASP%20Certification%20White%20Paper.doc White Paper.

Minoli, Daniel, E. Minoli. (1998). Web Commerce Technology Handbook. McGraw-Hill Companies Inc. New York, NY.

Network Associates Technology, Inc. (1996-1999). Gauntlet Firewall/VPN for WindowsNT Getting Started Guide v5.5. Network Associates Technology, Inc. Santa Clara, CA.

Thawte - A Verisign Company. www.thawte.com

© SANS Institute 2000 - 2005