ACNielsen Web Security

White Paper

Mike Ellsworth

U.S. Systems

October, 1997

ACNielsen Web Security

With the advent of BrokerNET in February, 1995, ACNielsen pioneered electronic report delivery using the World Wide Web. In order to ensure the security of BrokerNET, and later of SalesNET, we undertook several measures involving two areas of security:

- browser to Web server security,
- Web server to internal network (WAN) security.

Browser to Web server security involves all traffic between the user's Web browser and the ACNielsen Web server. What is currently offered in BrokerNET and SalesNET provides adequate security for our customers' use of these services. We can optionally offer enhanced security by using Netscape browsers and servers, and by implementing Secure Sockets Layer (SSL) encryption.

Web server to internal network security in the two existing products involves the use of our existing firewall to isolate traffic from the Internet, and provisions for one-way file transfers of information from the ACN WAN to the Web server. In future services, including services that offer interactive drill down into our data bases, new security schemes must be put in place to enable transactions (user requests) to traverse the firewall and be routed to the data base servers on our WAN.

This document describes the current state of our security set up as well as optional and planned security measures.

General Browser to Server Security Requirements

Complete browser to server security must provide the following services:

- Confidentiality of the HTTP transaction
- Authentication of the server/service.
- Authentication of the client/user.
- Integrity of the HTTP transaction

These services must be provided independently of each other. Currently, BrokerNET and SalesNET provide authentication of the client/user, and provide some measures to ensure the integrity of the HTTP transaction. At customer option, we can provide all four facets of browser to server security through the use of Secure Sockets Layer (SSL), described later in this document.

Confidentiality

If the need for confidentiality of the traffic between the browser and the server is high, the components must provide confidentiality of the HTTP transaction via encryption of the HTTP messages. In this case, the entire HTTP transaction must be considered private; thus, the HTTP headers and data objects of client requests and server responses, including the URL being accessed, must be confidential. ACNielsen does not currently support this level of confidentiality due to our belief that the risk of any traffic falling into the hands of a third party is small, and even smaller when you consider the number of people who could both intercept a transmission and derive any benefit from it.

Use of SSL would meet this requirement. SSL is described in a later section

Authentication

If the confidentiality of the service being provided is high or if it is a paid service, components must support the authentication of the HTTP server to the client and vice versa. This means that users can ascertain that the server is indeed the server they are expecting (service authentication), and the server can determine that the user is who they say they are (user authentication).

Service Authentication

Service authentication involves the server being able to assure the client that it is what is purports to be. A common way this is done is with a digital certificate issued by a third party that states the identity of the server. This certificate is exchanged with the client as a means of authenticating the service.

A side issue is support of the authentication of gatewayed services to the client. In this case, either the user or the service provider is behind a firewall or other proxy. In such arrangements, more than one user can appear to have an identical point of origin. For example, all users within the ACNielsen network appear to services on the Internet to be coming from ac.nielsen.com, because they all must pass through a common firewall to get to the Internet. The same type of problem can obtain if the service is behind a firewall. Thus, any authentication scheme cannot be based on the apparent address of origin of the user or the server.

Our current services are not proxied, and we depend on the domain name (acnielsen.com or brokernet.com) to authenticate our service to the user. We consider this to be sufficient, as the likelihood of another provider masquerading as ACNielsen is vanishingly small. However, this requirement would be fully met by implementing the SSL technology and the Netscape Commerce Server. In this method, ACNielsen would obtain a digital certificate from a third party that certifies we are who we say we are. This certificate becomes the “signature” of the site, and users’ browsers can be set up to authenticate the service based on receipt of this certificate.

User Authentication

There are many schemes to support the authentication of the user to the server. The most common involves use of user id and password. There are many problems with this type of authentication, not the least of which is that users tend to forget passwords, or write them down. ACNielsen’s existing Web services use a session key technique to ensure that, once a user has authenticated him or herself, they continue to be recognized during the session.

The problem of user authentication is compounded by the stateless nature of the Web. Rather than, say, a 3270 connection, in which a user logs on once, and remains connected to the computer, Web connections are fleeting. A connection is made, information is exchanged, and the connection is broken. The next connection looks just like a new connection to the Web server, and herein lies the problem. We can ask people to log on, but then each page they request subsequently looks like a new request and requires authentication.

Many Web services handle this through a server-based authentication scheme that allows for a single log in. After the user logs in, the user id and password are stored in the browser and passed back to the server with each request. We do not feel that this is a good method of authentication for our type of services, since confidential information (user id and password) is exchanged in the clear many times during a session. If all traffic were encrypted using SSL, this method becomes more acceptable.

ACNielsen’s Session Key Methodology

To overcome this limitation, we developed the session key methodology. Each user in the system has a user id and a password, which is part of their user profile. Using the user profile, we can perform many types of authentication, including controlling access to various subsets of the service. For example, a customer may want to limit access to particular markets to only those sales people servicing those markets.

The user’s password is stored in the profile in encrypted form. When the user first loads the main service page, the system generates a unique session key which consists of random numbers and letters. When they enter their user id and password, the password is encrypted and compared to the stored password. If it is a match, the user id, password, and initial session key are combined to form a unique session key. This key is embedded in all pages returned to the user. If a user request comes to the server with a valid key, the request is honored. If the user does not use the service for more than 30 minutes, the session key expires, and the user must log back on.

Each page in the system is generated on the fly and no pages exist until requested, which adds another layer of security. Users cannot bookmark a particular page and return to it later due to this scheme.

Netscape's Cookies Methodology

A technological solution developed by Netscape called cookies is very similar to our session key methodology. Cookies can be used in conjunction with password authentication or in place of it, although use of cookies alone is not recommended for true electronic commerce.

Third party vendors of Web applications such as Information Advantage have adapted the password and cookies method to perform user authentication. Once the user enters the user id and password, the server sends a cookie to the browser, which stores it on the user's hard drive. Then, each time a user presents a request to the server, the server asks the browser for the cookie information. Cookies can be set to expire after a period of time. A disadvantage of this system lies in its storage of potentially sensitive information (in the form of cookies) on the user's hard drive, which may not be secured. There are a variety of privacy objections to this methodology as well.

Netscape has recently enhanced the cookie concept by including Sun Microsystems' Java language in Netscape's Personal Workspace operating environment. In Personal Workspace, users create a profile of themselves in the cookie section of the Navigator client, which details exactly what information, reference tools and applications they wish to receive. The cookie is then sent to the Netscape server, which delivers back the selected preferences in the form of a full-screen operating system.

Consumers use cookies to automatically identify themselves and pick personal content preferences for future visits. If widely accepted by consumers, cookies could become the de facto standard for identifying users on a Web site.

The use by ACNielsen of cookies for user authentication is probably redundant to our existing scheme. However, depending on how the Personal Workspace concept evolves, we may want to take a look at this technology again.

Integrity

To fulfill this requirement, a service must provide assurance of the integrity of the HTTP transaction, including the HTTP headers and data objects of both client requests and server responses.

ACNielsen's scheme of creating pages on the fly partially satisfies this requirement. However, only a totally encrypted session methodology such as SSL can completely guarantee integrity of the transaction. We believe our methodology is sufficient given the sensitivity of the data and can implement SSL technology for customers who desire more.

Secure Sockets Layer (SSL)

Netscape Communications has designed and specified a protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP. This security protocol, called Secure Sockets Layer (SSL), provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

Netscape Navigator

All versions of Netscape Navigator browser (beginning with 0.93 for Windows, Mac, and UNIX variants) have integrated support for SSL. This support is implemented as follows:

- Netscape Navigator supports a new URL access method, "https", for connecting to HTTP servers using SSL.
- Netscape Navigator is approved for export by the United States Government. Because of export restrictions, Netscape Navigator is limited to a 40-bit key size for the RC4 stream encryption algorithm

(the encryption algorithm used by Netscape Navigator's implementation of SSL). A message encrypted with 40-bit RC4 will take on average 64 MIPS-years to break (a 64-MIPS computer will need a year of dedicated processor time to break the message's encryption). This is not military-grade security, but the effort required to break any given "https" data exchange is definitely nontrivial.
- Netscape Navigator supports the standard X.509 cryptographic certificate format within SSL. Currently, Netscape only supports use of server certificates; clients may not (yet) have certificates.

Netscape Commerce Server

Netscape Commerce Server implements server-side support for HTTP over SSL, including support for acquiring a server certificate and communicating securely with SSL-enabled browsers like Netscape Navigator

U.S.-only versions of both Netscape Navigator and Netscape Commerce Server with high-level security support, including 128-bit RC4 are available

SSL provides a security "handshake" that is used to initiate the TCP/IP connection. This handshake results in the client and server agreeing on the level of security they will use, and fulfills any authentication requirements for the connection. Thereafter, SSL's only role is to encrypt and decrypt the bytestream of the application protocol being used. This means that all the information in both the HTTP request and the HTTP response are fully encrypted, including the URL the client is requesting, any submitted form contents (including things like credit card numbers), any HTTP access authorization information (usernames and passwords), and all the data returned from the server to the client.

Browsers that do not implement support for HTTP over SSL will naturally not be able to access "https" URLs.

The Netscape client and server technology described here is used by various third party vendors Use of these vendors will naturally require us to adopt the Netscape client and the Netscape Commerce Server as ACNielsen standards. This would allow us to offer enhanced security to our customers at their request.

General Server to WAN Security Requirements

Complete Web server to WAN security must provide the following services:

- Confidentiality of the transaction
- Authentication of the client/user.
- Integrity of the HTTP transaction
- Protection of service components
    - Web Server
    - Gateway/firewall machine
    - Wide Area Network
    - Service delivery machine

These services must be provided independently of each other. Since they are not transaction-oriented services, BrokerNET and SalesNET aren’t too concerned about protection of the WAN or any transaction issues. Information is loaded into these services by a one-way FTP connection that allows machines in production to transfer files to the Web server, but does not allow the Web server to transfer information back through the corporate firewall. These services rely on the corporate firewall to protect the WAN.

The following sections address future needs and plans to meet those needs, enabling ACNielsen to offer interactive, Web-based information delivery services with world class security.

Confidentiality of the Transaction

Any transaction requested by a user, to run a report, or drill down into a data base, for example, must be held confidential. The transaction must not be observable by third parties, nor should the log or any accounting of the transaction be exposed to the Internet.

Confidentiality is enhanced by disallowing log ins or FTP sessions to the Web server. However, ACNielsen does not address the issue of confidentiality. Use of SSL would resolve this issue.

Authentication of the Client/User

ACNielsen advocates use of user id and password authentication. This solution could be enhanced by the use of SSL.

Integrity of the HTTP Transaction

ACNielsen believes that sufficient measures have been taken to adequately ensure the integrity of the HTTP transaction. Use of SSL could improve these measures.

Protection of Service Components

This is probably the most important aspect of Web server to WAN security. There are four types of threats we need to defend against:

- Threats against the Web Server (and hosting machine)
- Threats against the gateway/firewall
- Threats against the WAN
- Threats against the service delivery machine (including theft of service)

Web Server

The Web Server is the most vulnerable piece of the puzzle. Although much progress has been made in Web Server security over the last year, this is still an immature technology. The chances of a successful attack on a Web Server are much higher than on any other component.

Possible threats include overwhelming some aspect of the server’s operations to gain access to the hosting machine as well as malicious overwhelming of the Web Server itself with spurious requests, causing degradation of service to paying customers.

Since no remote log ins are available on the machine, and since it is isolated from the rest of the network by a firewall, the consequences of an intrusion on the Web server are limited.

Defense against intentional overwhelming of the service by unauthorized users is much harder, and bears study. Perhaps we need some mechanism to automatically reject attempts to connect by users that fit a certain profile (more than 100 requests in the last minute, for example.)

Gateway/Firewall Machine

Compromising the gateway or the corporate firewall would be a disastrous occurrence, obviously. Consideration of the security of the corporate firewall machine is beyond the scope of this document. However, if we adopt Virtual Vault, we will be in effect opening another gateway into our WAN, and that gateway must be fortified.

The compartmentalization of the public and private sides of the HP machine ensures that any damage can be limited to the public side if we accept the premise that Secure HP UX does effectively isolate the private side from the public side. However, since the compartments share the same physical machine, it is conceivable that an attack on the public side could affect the private side.

Wide Area Network

Protection of the WAN must be the number one concern. The gateway machine must operate in a fail-safe mode. If the machine goes down or is attacked, there must be no possibility that an intruder could slip into the WAN from that point

Service delivery machine

Attacks on the service delivery machine don’t necessarily imply a breach of security on the WAN since they include theft of service. However, should the WAN be compromised, the service delivery machine should be adequately secured with proper user account and password protection.

Summary

It is my opinion that security measures in place in existing services offer adequate protection of both ACNielsen and our customers. At customer request, such measures could be strengthened by the use of SSL