PrivyLink Internet Application Security Environment*

The End-to-end Security Solution for Internet Applications

September 2003

The potential business advantages of the Internet are immense. Organisations can leverage on the Internet to access new clients, open new markets and provide a new cost-effective channel for service delivery and, partners and customers communications. Services like on-line banking, stock-broking, electronic commerce and marketplaces, telecommuting accesses and electronic mail, are prime examples of this potential.

The foremost factor preventing many organisations from taking advantage of these business opportunities in this prevalent *e-Economy* are customer concerns over the security risks and exposures in the Internet. Data transmitted over uncharted network, such as the Internet, is vulnerable to interception, electronic vandalism, theft and alteration.

Security mechanisms are required to protect these high-value data from all malicious attempts across the open network and are imperative to ensure the Return-On-Investment of all Internet Pure-Plays or "click-and-mortar" businesses.

SSL and Secure HTTP (*SHTTP*) are two widely adopted security measures used to protect the channel for data exchange, with SSL currently being the most prevalent. However, both have their respective shortcomings.

SSL being an open protocol is often the subject of cryptanalyst and its weakness against active attacks as reported in the recent months has alarmed organizations using it for their application data security. In addition, SSL provides only session-based protection and has no data persistency, and its protection end-points are the browser and the web-

* The information contained in this document represents the current view of PrivyLink International Ltd, and is correct as of the date of publication. This document is for information purposes only. PrivyLink International Ltd makes no warranties, express or implied, in this document. Information in this document is subject to change without notice, and does not represent a commitment on the part of PrivyLink International Ltd. PrivyLink International Ltd cannot guarantee the accuracy of any information presented after the date of publication.

server. However, most networks today are multi-tiered and the data end-point is usually the application server or the host machine. Internal network security risk is not addressed. Thus, SSL no doubt is a valuable step towards practical communications security for Internet applications; it is insufficient to satisfy most organizations security requirement for their application data.

Threats to SHTTP are similar to those against SSL[1] with the default operation mode of SHTTP being substantially more resistant than that of SSL. However, its limited use (*supported only by Secure Mosaic from EIT*) and weakness in key exchange render it inappropriate as the choice security mechanism.

Purpose

Internet applications are in wide spread use nowadays. Organisations will leverage on the Internet and provide more cost-effectively channels for data communications in terms of business world. Security becomes a significant concern to be considered for the decision making of the organisations.

This paper describes the concept of the Internet Application Security Environment, its business and security benefits, and its deployment scenarios.

We will first look at the security requirements of most organisations and the current security technologies being deployed. We will then examine the security inadequacies in these security technologies and demonstrate how the Internet Application Security Environment (IASE) overcomes them to deliver complete end-to-end application layer security to the application data.

End-to-end Security Requirements for Internet Applications

Focusing on most Internet application requirements, organisations need to at least satisfy the following application security requirements:

1. Identification and authentication – to enable the application to establish the identity of a user over the Internet, and authenticate the claimed identity to ensure that it can be trusted to provide the requested access to information and resources within the organisation and potentially, its business alliances.
2. Data integrity protection – to ensure that the contents of the application data have not been corrupted or tampered with during transit from the sender to the recipient through the network.
3. Data confidentiality protection – to ensure that the contents of the application data (if it is sensitive in nature) are kept private or confidential throughout the process.

[1] http://www.homeport.org/~adam/shttp.html

Business Acceptance Criteria

In addition to achieving the above security requirements, the desired solution needs to ensure that its implementation exhibits a number of important characteristics that will meet the business needs of the applications concerned.

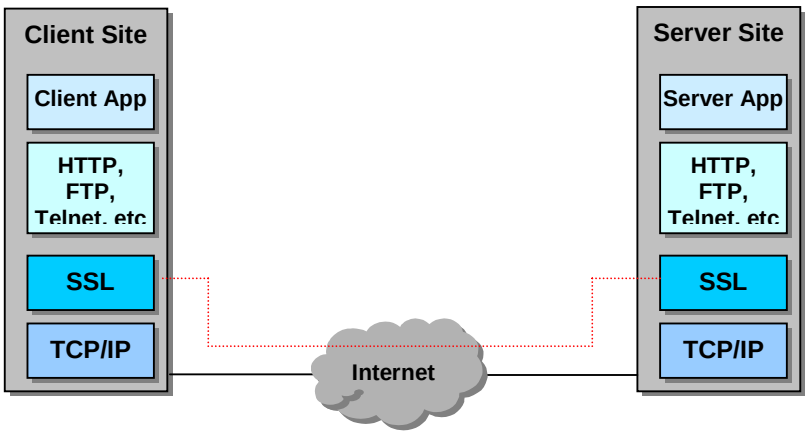
1. Usability. As far as possible, the solution should not require intervention of the users or administrators at both ends of the system i.e. it must be transparent.
2. Affordability, so that the initial investment and ongoing operation cost relating to managing the security risk of Internet application services are justifiable from the business benefits perspective.
3. Low overhead and high throughput, which are important factors on the usability of the end products. The security mechanisms at both ends of the system should produce the desired output within reasonable time period acceptable in the Internet environment. The overheads and performance, if not managed, would result in undue delays, which will restrict the use of the solution, and end-user acceptability of the application system as a whole.

SSL Security Issues

TCP/IP protocol is the de-facto communication protocol for connecting millions of machine together, thereby creating the Internet. However, TCP/IP was not designed with security in mind; hence it is vulnerable to network eavesdropping. When confidential documents are transmitted from the Web server to the browser, or when the end-user sends private information back to the server inside a fill-out form, someone may be listening in.

Thus, to overcome the lack of security in the original communication protocol, Secure Sockets Layer or SSL was developed. SSL is the Internet security protocol (over TCP/IP) for point-to-point connections. It provides protection against eavesdropping, tampering, and forgery. Clients and servers are able to establish a secure link across the Internet to protect the information being sent and received. Let us examine the issues in greater detail in the remaining section.

SSL and OSI Layer



SSL Version 3.0 was first published by Netscape Communications Corporation (TLS version 1.0, defined in RFC 2246, was based on SSL Version 3.0). It is a low-level encryption scheme used to encrypt network data transmitted in higher-level protocols such as HTTP, NNTP and FTP. The SSL protocol includes provisions for server authentication (verifying the server's identity to the client), encryption of data streams in transit, optional client authentication (verifying the client's identity to the server) and message integrity checking via MACing.

SSL Approach and Issues

Businesses today are putting more applications onto the web environment and due to high transaction volume; web services are no longer deployed on a singe machine. In fact, most web services are now enabled with web and application servers, with web servers acting as delivery channels and application servers for processing application requests. Figure 1 illustrates such a system set up.

As shown in Figure 1, such an implementation leaves us with security gaps, which are potential issues in implementation. An organization's use of the Secure Socket Layer (SSL) version 3.0 protocol protects the Internet channel, but does not secure the end-to-end application channel.

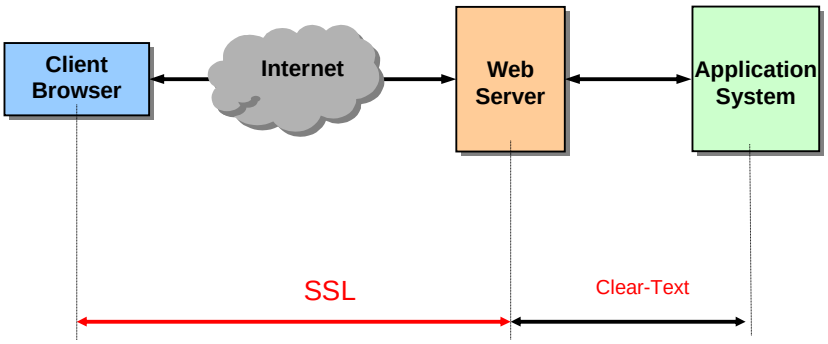


Figure 1: SSL-based Web Deployment

SSL performs information encryption on a standard browser-to-server transaction. It only secures the connection to the web server, thus securing transactions partially. Unfortunately, securing the network borders is not enough. Data flowing across the web server remains vulnerable to internal risks or third-party risks in case of an outsourced web service. The use of SSL alone without application layer security therefore creates a false sense of security and does not address the true application security requirements.

Security Inadequacies of SSL for end-to-end security

An obvious concern in SSL is that it only secures the session, it does not secure any actual transaction. This means if someone does steal another's credit card number and use it online, it is almost impossible to prove that it was not actually that person who issued the order. SSL does allow for the

client to authenticate to the server, however very few people have digital certificates compatible with this and most certificate vendor do not completely verify the identity of the certificate applicant. In addition, such client-to-server authentication only authenticates the communicating entity and not user at the application level.

There are newer protocols and systems that allow for two parties to safely conduct transactions with all these features. Thus, SSL alone is inadequate to secure Internet based transaction systems.

IASE

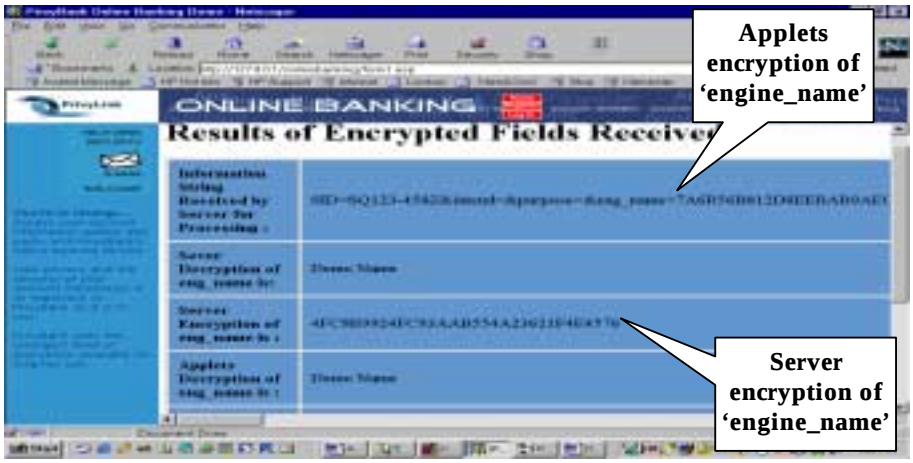
The IASE is designed to address the security requirements of web-based applications. The deployment of IASE will enable organisations to secure their valuable data end-to-end and allow secure user authentication over the Internet.

The following section illustrates how the Internet Application Security Environment solution can be used for identifying and authenticating user over the Internet and how the IASE Security Applet ensures the confidentiality and integrity of user information by encryption.

User Authentication

As users are authenticated over open networks, most available authentication protocols are not suitable for deployment. The IASE deploys a unique challenge-response authentication method to ensure that derivation of user passwords obtained during data transmission is virtually impossible. The one-time challenge feature prevents intruders from performing replay attack on the system. IASE makes use of strong cryptographic techniques incorporating128-bit DES and 1024-bit RSA encryption algorithms. Hence, with IASE, users can be assured that their passwords will not land in the wrong hands.

The screen capture below shows that the encrypted string obtained for the ‘engine_name’ is different when encrypted on the server side and the browser side. However both are able to decrypt the string to obtain the original ‘engine_name’.



Below shows a sample code segment, which downloads the IASE security applet to the browser.

```
<applet name="TrustFieldExtApp" codebase="./Demo"
code="TrustFieldExtApp.class" width="1" height="1" VIEWASTEXT>

<param name="Challenge" value="ABC4567890123456789012345678901 2">

<param name="SID" value="SQ123-458Z">

</applet>
```

Data Encryption

Data confidentiality is one of the most important aspects of security. Authentication may have conclusively identified the participants in a transaction, but does not ensure the confidentiality of the sensitive data that is being transmitted. To ensure the confidentiality of the information, the data must be encrypted. Encryption and decryption is the process of protecting information from being tampered from unauthorised parties.

IASE provides a two-way encryption data security applet using Java technology. The applet delivers a secure way for exchanging sensitive information between clients and the organisation over Internet. It uses sophisticated Java technologies to encrypt and transmit client information securely over WWW.

IASE and Cryptographic Key Server

PrivyLink's Cryptographic Key Server is used to manage IASE system keys and user passwords to provide maximum security. It is a hardware-based key management server that provides security functionality to Internet, Intranet, Extranet, and enterprise infrastructure applications. It safeguards sensitive private key information with strong physical and logical security, and offloads computationally intensive public key operations from the server. A combination of these products, applied to your application, eliminates the significant bottlenecks and risks associated with software security processing.

IASE SDK

Another component of IASE is the software development kit (SDK). The IASE SDK provides the server end of the security functionality required for supporting end-to-end security for the Internet application. It includes:

- Secure session establishment with IASE client applet;
- Secure user authentication;
- Secure data encryption/decryption; and
- Secure integration with IASE Cryptographic Key Server (CKS) for secure key management.

The IASE SDK enables developers to build and integrate IASE-compliant applications with minimal efforts. Developers simply need to identify the information required to be secured and apply the relevant security application application interfaces (API) available.

PrivyLink's IASE provides developers with an expert product that includes everything needed for delivering a ***TRUE*** end-to-end security application. This means corporations can make their deadlines without having to become cryptographic experts.

Deployment Scenarios

This section illustrates the scenario where the IASE can be deployed to secure an Internet Application Environment.

IASE deployment is really simple. Following are the steps that may be taken.

1. Minor modification to main web page.
2. Replacement of authentication method with IASE authentication API.
3. Identification of sensitive parameters and applying the relevant security APIs.

Together with the deployment of the Cryptographic Key Server (CKS), IASE is ready to protect the sensitive information exchanged between the Client and the Application System. The IASE can co-exist with SSL seamlessly. Figure 2 illustrates how IASE is being deployed.

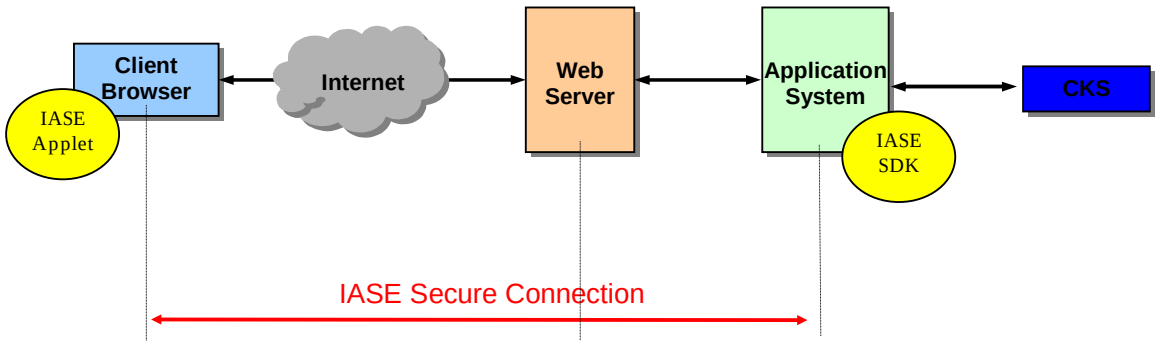


Figure 2: IASE-based Web Deployment

Benefits

Convenience

Organisations need not explicitly distribute encryption software to clients; hence the service can be deployed without having to invest in establishing security infrastructure to support the operations.

Standard Compliance

The IASE uses standard based 3DES for symmetric encryption and RSA for asymmetric encryption and supports full strength key length at 128 bit and 1024 bit respectively.

Flexible

The IASE modular design allows the change of underlying cryptographic algorithms transparently on a regular basis and also for organization to respond efficiently to changes in systems security technology development. Thus ensuring their returns on investment in IASE.

Operating Environment

- The IASE Server module is currently supported on SUN Solaris and Windows 9x/NT operating systems.
- IASE supports CGI/C, ASP scripting and Java Servlets, and support application server such as iPlanet Application Server.
- IASE Client module supports both Microsoft Internet Explorer version 3.x and above, and Netscape Navigator 4.x and above.
- The Cryptographic Key Server supports the IASE natively for better server-side security.

Optional Features

According to the organization's need, IASE can be deployed with optional features:

- ActiveX component for Windows CE platform
- Dynamic Pin Pad for enhanced PIN security management
- PKI Integration
- Stress Test Module for server web application benchmarking

Please direct all enquiries for information on the above options to the respective sales contacts provided below.

Conclusion

In conclusion, IASE does not only address organization's end-to-end security needs for their application data, it also afford a strong challenge-response based authentication mechanism for user identification and

authentication. With its native support for server-side cryptographic key server, such as the CKS, the IASE is truly ***the*** end-to-end security solution for all Internet applications.

About PrivyLink

Founded in 1997, PrivyLink is a response to strong industrial demands for high assurance delivery channel for electronic transactions, especially in the government and financial sectors. PrivyLink offers a comprehensive suite of software and hardware solutions to address end-to-end e-Security of today and tomorrow's businesses in the e-Commerce, e-Business, and e-Marketplace arenas.