



# Web Application Security



## United Security Providers Whitepaper

20. November 2006  
Hans-Peter Waldegger  
Version 1.0



## Contents

<b>Contact .....</b>	<b>3</b>
<b>Web security challenges .....</b>	<b>4</b>
Worldwide accessibility .....	4
Sensitive data.....	4
Organized criminals.....	4
Operational nightmare .....	4
User convenience .....	4
Only the paranoids will survive.....	5
Most common vulnerabilities.....	6
The patch dilemma.....	6
<b>Countermeasures.....</b>	<b>8</b>
Protective Components .....	8
Web Application Firewalls .....	9
<b>Secure Entry Server® .....</b>	<b>11</b>
Security.....	11
Single Sign-on .....	12
Knowing/recognizing the user .....	15
Better performance and higher availability .....	16
Solution for the patch dilemma .....	16
Tamper proven protection .....	16
<b>Use cases .....</b>	<b>18</b>
Mail access for field workers .....	18
ERP connection for remote agencies.....	18
Shield your valuable web applications .....	18
User authentication for sensitive data .....	19
Re-Authentication for critical transactions .....	19
Single Sign-on for portals.....	19
Wiki or blog communities .....	20
Web Services.....	20
Online questionnaires .....	20
<b>Conclusion .....</b>	<b>21</b>



## Contact

Product Manager SES

Hans-Peter Waldegger  
United Security Providers  
Förrlibuckstrasse 220  
Postfach  
8031 Zürich  
[hans-peter.waldegger@united-security-providers.ch](mailto:hans-peter.waldegger@united-security-providers.ch)



## Web security challenges

### Worldwide accessibility

Today, 24/7 worldwide accessibility of data and applications is crucial for most businesses. The Internet is a perfect enabler but also a home for spys, cyber criminals and script kiddies.

How do you protect your applications from hackers without constraining your legitimate users?

### Sensitive data

Web applications become increasingly popular exchanging tremendous amounts of data. This data also includes sensitive items or data protected by privacy laws - such as personal, medical and financial information.

Can your application comply with all relevant access and audit regulations?

### Organized criminals

Organized criminals and contract hackers steal and trade company data. Apart from the value of the stolen data, the damage to the corporate image is invaluable.

How can you reduce the security risks and simultaneously keep the flexibility to add new or extend existing web applications?

### Operational nightmare

Only strictly monitored and frequently updated systems can resist all the attacks.

How can you regularly patch the applications and operating systems while fulfilling service level agreements?

### User convenience

Security and user convenience often are a tradeoff.

How can you prevent your users from writing down or sharing their passwords?



## Risks and Vulnerabilities

### Only the paranoids will survive

Computers connected directly to the Internet are exposed to a great danger of getting attacked. Experts estimate computers to be attacked with a probability of 90% within the first hour they are attached to the Internet. The random attacks of earlier hacker generations have been replaced by commercially driven, coordinated and automated attacks by organized criminals who have recognized the ability to make money using the Internet.

Five years ago, the majority of attacks targeted operating systems and Internet services like web servers and mail systems. Security professionals have invested a lot of time identifying and correcting vulnerabilities in operating systems and server administration setup. As a result, most of today's servers are hardened and much more secure than they used to be.

In 2005, most attacks concentrated on application programs: 69 percent of the reported vulnerabilities<sup>1</sup> affected Web application technologies, a 15 percent increase over the previous period. Web application technologies, which rely on a browser for their user interface, present an easier target for attackers due to their availability over commonly allowed protocols such as HTTP.

#### Intrusion at DoD

The Department of Defense (DoD) announced on April 28, 2006 that routine monitoring detected unusual activity on one of the TRICARE Management Activity's (TMA) public servers. Investigation of the activity led to the discovery that an intrusion had occurred and information was compromised.

DOD News Release  
No. 375-06

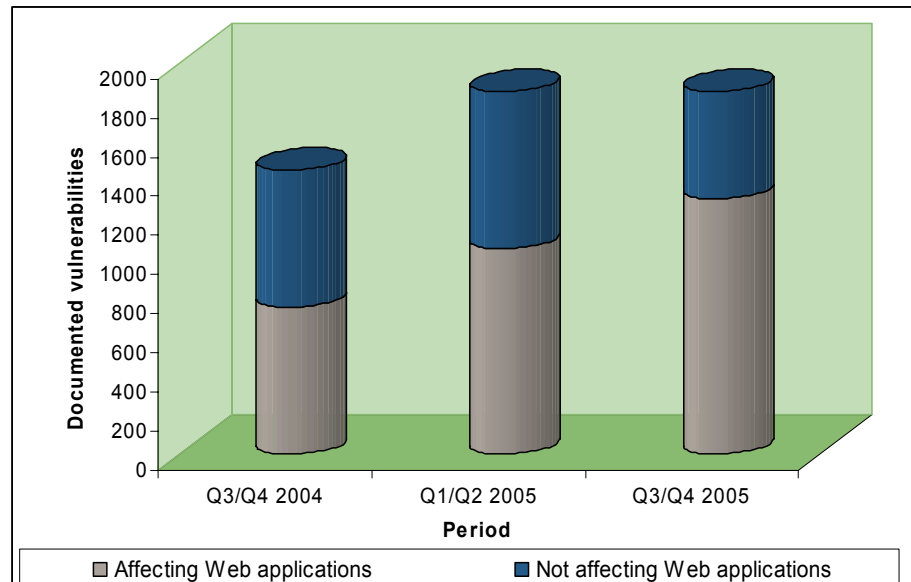


Figure 1: Vulnerabilities in Web Applications

<sup>1</sup> Source: Symantec



Unprotected web applications won't survive the first day on the Internet. If you don't have the appropriate tools in place, you will not even notice that your application has been hacked.

## Most common vulnerabilities

The "Open Web Application Security Project" (OWASP), a foundation dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted, publishes since 2003 a list of security problems. The OWASP top ten list is the security experts' consensus of the most critical web security vulnerabilities that require immediate remediation (see Table 1).

### The patch dilemma

In 2005, an average about 6 days elapsed between the announcement of a vulnerability and the release of an associated exploit. An average of 49 days elapsed between the disclosure of a vulnerability and the release of a vendor-supplied patch. Consequently, enterprises and consumers may be susceptible to potential attack for at least 43 days, highlighting the need for users to patch systems or take other protective measures as soon as possible.

#### Cross Site Scripting

Security labs report that the Samsung Telecom website is hosting malicious code. The site has been hosting a number install malicious code on end-users' machines.

The most current code, which is still available for download, is a Trojan Horse that attempts to disable anti-virus programs, modify registry keys, download additional files, and log keystrokes when connecting to banking websites.

Websense®  
September 06, 2006



Table 1: OWASP Top Ten (OWASP)

<b>A1</b>	<b>Unvalidated Input</b>	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
<b>A2</b>	<b>Broken Access Control</b>	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
<b>A3</b>	<b>Broken Authentication and Session Management</b>	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
<b>A4</b>	<b>Cross Site Scripting (XSS) Flaws</b>	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
<b>A5</b>	<b>Buffer Overflows</b>	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
<b>A6</b>	<b>Injection Flaws</b>	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
<b>A7</b>	<b>Improper Error Handling</b>	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
<b>A8</b>	<b>Insecure Storage</b>	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
<b>A9</b>	<b>Denial of Service</b>	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
<b>A10</b>	<b>Insecure Configuration Management</b>	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

**Broken authentication**

The Internet-Shops of the German warehouses "Quelle" and "Neckerman" had a serious security hole. It allowed attackers to read customer files or even to order goods on somebody else's expenses.

This vulnerability was not detected until a hacker informed the press.

Wirtschaftswoche  
September 08, 2006



## Countermeasures

### Protective Components

The occurrence of attacks is neither new nor alarming. A lot of companies are successfully facing these problems for many years. Different concepts and products have been designed to protect servers exposed to the Internet.

#### Broken access control

The 2006 and 2007 versions of Panda's Internet Security Suite enable users to escalate their privileges.

Security testers were able to replace the Web-Proxy and gain system privileges. Any malware which slipped through Panda's filter would be able to embed itself deep into the system using this method.

Heise-Security  
September 09, 2006

- **Network zoning**  
A demilitarized network zone (DMZ) is a special network segment, where all servers and network components with connections to the Internet are collected.  
*It is like the entry hall in your office.*
- **Bastion hosts**  
Bastion hosts are specialized computers that stand in front of the DMZ and are the primary contact for external computers requesting a service. They are fully exposed to attacks and need special protection mechanisms.  
*Think of a bastion host as being a cash desk of a bank.*
- **Firewalls**  
Firewalls are network components that allow or prohibit network traffic from PCs on the Internet to a defined subset of services available in your DMZ.  
*A firewall is like a doorman, restricting the access to some office areas, contact persons or office hours.*
- **Reverse-Proxies or Application Gateways**  
Proxy systems are used to prevent direct connections from one system to another. They increase the security by acting as small agents giving access to some services of a powerful system but shielding the complete system. While proxies are used to connect internal systems to the Internet, reverse-proxies forward requests from the Internet to internal services.  
*A waiter may be seen as a proxy for a chef working in the kitchen. The waiter makes sure you select a predefined dish and forwards your request to the chef. Only he is allowed to enter the kitchen.*
- **Intrusion Detection and Prevention Systems**  
Intrusion detection systems scan the network for anomalies in the traffic and for suspicious data. They raise an alarm (detection) or block the request (prevention).  
*It is like a security guard watching the people entering a building and keeping away people that do not comply with certain rules.*
- **Web Application Firewall (WAF)**  
A conventional firewall reliably ensures that the hacker cannot use any ports or protocols for his attack unused by applications. Within these limits, however, web applications have to fend for themselves when it comes to thwarting attacks. A web application firewall (WAF),



which has little to do with a conventional firewall, fundamentally alters this situation. It does not just monitor whether the traffic to a target system uses the right protocol or not. A WAF goes further and integrally monitors the whole content of every inquiry.

*If a firewall can be compared with a doorman, then a WAF is a kind of bodyguard, taster, lawyer and fiduciary, with added close-combat training.*

### Buffer overflows

A vulnerability found in the way the ICQ Pro 2003b client handles incoming message lengths could lead to denial of service attacks and remote compromise of systems running vulnerable versions of the client.

A heap overflow vulnerability was found in the ICQ Pro 2003b build #3916 IM client. The problem derives from the way the vulnerable client handles the length of a specific type of message received from other clients.

CoreLabs Advisory  
September 07, 2006

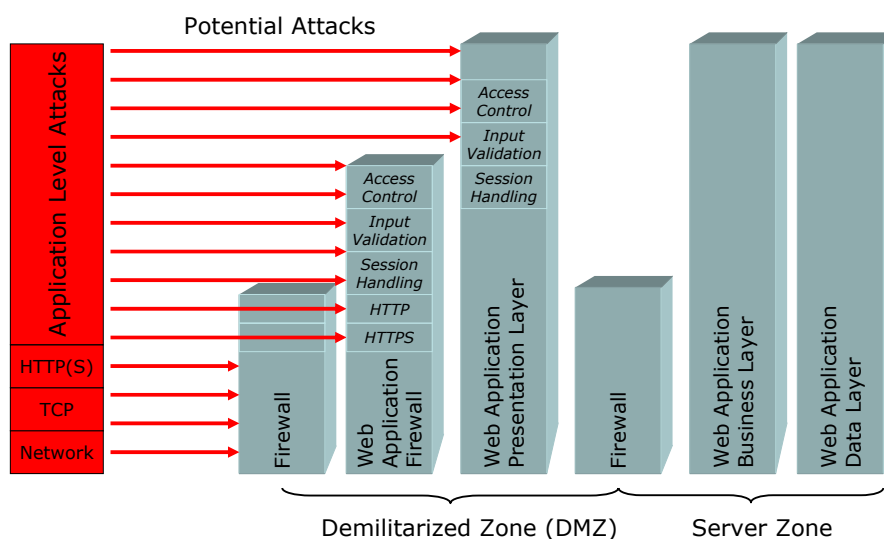


Figure 2: Components shielding web applications

## Web Application Firewalls

The main task of Web Application Firewalls is traffic inspection using a technique called 'Deep Packet Inspection'. They look at every request and response within the HTTP/HTTPS/SOAP/XML-RPC/Web Service layers. Some WAFs look for certain 'attack signatures' to try to identify a specific attack that an intruder may be sending, while others look for abnormal behaviour that doesn't fit the website's normal traffic patterns.

In order to optimize defence against attacks, an architecture that allows access to all the data traffic and, at the same time, enforces a clear separation between the data and the application, is needed. WAFs must be placed inline in the DMZ, upstream of all web applications. They are installed before the web application server and thus prevent direct unprotected access to the application server by a user. In order for the WAF to also inspect the encrypted data exchange, it must either form the end-point of the SSL encryption or have access to a copy of the encrypting key.

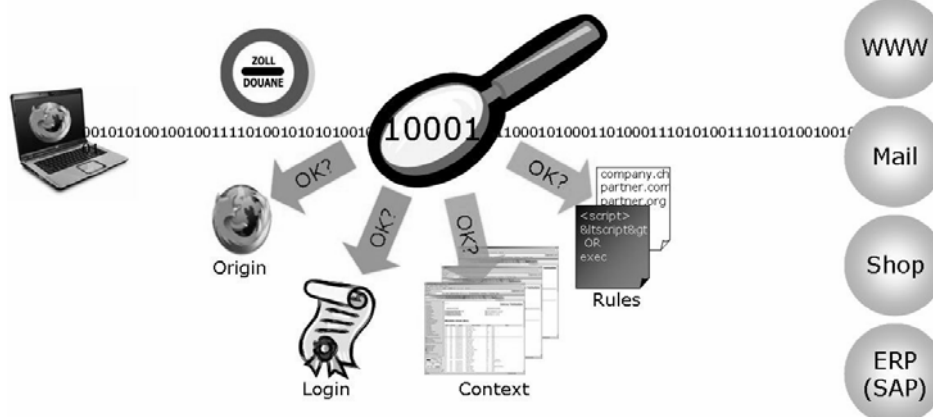


Figure 3: Secure Entry Server® inspects data transfer

**Insecure Configuration**

SANS reported Botnets being created out of vulnerabilities found in Pmwiki. The Pmwiki exploit can only be used if you have "Register\_globals" turned to "On" in your php installation.

SANS Internet Storm Center  
September 05, 2006

In this way, each browser no longer communicates directly with the application server, but instead simply with the WAF, which, as before, checks the inquiry for samples and anomalies. In addition, however, contrary to an IPS, it also checks the inquiry in the context of the user session. For example, form parameters will be blocked if these are sent to the server without the server having asked the client beforehand. Such data manipulations constitute the most frequent kind of attack, but are neither recognized as such by classic firewalls nor by IPSs. The reason is that only a false context, i.e. not the protocol nor the isolated individual content, allows a dangerous intention to be recognized.

A typical reverse-proxy-based WAF authenticates and monitors all incoming inquiries, and forwards these to the back-end systems in case of appropriate authority.

However, Web Application Firewalls are not limited to packet inspection. Fully fledged WAFs also offer various authentication mechanisms, recording features and optimize the overall system performance through e.g. load-balancing, fail-over and data compression.



## Secure Entry Server®

The Secure Entry Server® (SES) is a reverse-proxy based web application firewall. It can be used as a bastion host in your firewall environment to secure the access to your web applications. In addition to security features, the Secure Entry Server® suite offers web single sign-on (authentication) and protected access to different network security zones (authorisation). These features also make it a primary choice for portal based enterprise SSO.

### Unvalidated Input

SAP-DB/MaxDB is a heavy-duty, SAP-certified open source database targeted for large mySAP Business Suite environments and other applications that require maximum enterprise-level database functionality and complements the MySQL database server.

Due to an input validation error, it is possible to execute arbitrary code with the privileges of the 'wahttp' process by sending a malformed HTTP request. Authentication is not required for successful exploitation to occur.

Symantec  
August 29, 2006

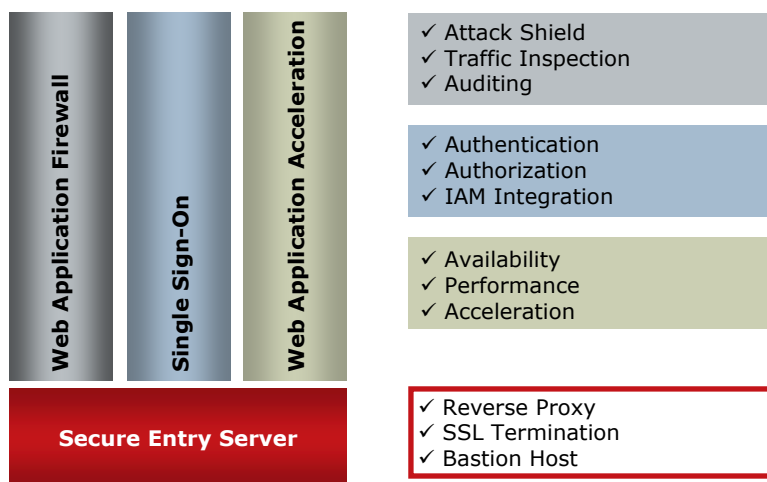


Figure 4: Benefits of the Secure Entry Server® (SES)

## Security

The Secure Entry Server® (SES) is a full fledged Web Application Firewall that examines all data transferred to and from web applications. In addition to this deep packet inspection, the SES contains many mechanisms to either block attacks completely or limit the effect of malicious data. Table 2 on page 13 gives a brief overview of the concepts used to defend the web server against the top ten OWASP vulnerabilities.



## Single Sign-on

User authentication takes place once only and thereafter allows users to jump backwards and forwards between different applications without repeated log-in procedures. Hence, for users, this means a wonderful, previously lacking experience, i.e. an improvement for operators provides increased security for the company at the same time.

For the convenience of system integrators the Secure Entry Server<sup>®</sup> uses an adaptive application integration (AAI) logic that allows to attach most system without changing anything in the existing web applications. To support integration of federated systems and application programmers extending legacy applications with web based back ends, the SES offers a toolkit including various features to retrieve and share digital identities and enable principal delegation.

### Denial of Service

The Cisco PIX 500, ASA 5500 and the Firewall Services Module (FWSM) are affected by a software bug that may cause the password to be changed without user intervention.

Unauthorized users can take advantage of this bug to try to gain access to a device. In addition, authorized users can be locked out and lose the ability to manage the affected device.

Cisco Security  
Advisory  
August 23, 2006



Table 2:SES concepts against OWASP Top Ten vulnerabilities

<b>A1</b>	<b>Unvalidated Input</b>	<p>The Secure Entry Server® uses extendable filter sets to examine the incoming and outgoing traffic. The configuration includes - but is not limited to - minimal length, maximal length, data type and character set restrictions for parameters and form data. Rules can be either applicable to all web servers (base rules) or specific to an application (specific rules).</p> <p>Additionally, all URLs presented to the client browser may be encrypted to additionally reduce the risk of parameter tampering and forceful browsing.</p>
<b>A2</b>	<b>Broken Access Control</b>	<p>The SES adds an additional point of access control enforcement in front of your web applications. Anonymous users may only access the public content area. Access to restricted areas is only granted to authenticated users. Optionally, the Secure Entry Server® may also restrict access to applications only to users belonging to a specific group. Finer grained access control remains fully in control of the web applications.</p>
<b>A3</b>	<b>Broken Authentication and Session Management</b>	<p>Different web servers use different techniques to carry connection and authentication information forward from one user request to the next. Some use cookies, others store a session ID in the URL. If a malicious user succeeds in stealing the cookie or session ID, he can incorporate the legitimate user's identity.</p> <p>The Secure Entry Server® stores cookies of all client connections in his own local cookie store and makes it impossible for attackers to steal application cookies. It further ensures that user requests are all issued by the same source identified by one or more of the following parameters: The user's IP address (login, current, last) or domain name, the browser type, the SSL session ID (login, current, last) and/or using a unique session ID generated by the SES.</p> <p>These features prevent session stealing without locking out authorized users: United Security Providers' customers experience a false negative rate that is lower than 0.05%!</p> <p>Additionally, the Secure Entry Server® offers centralized authentication with Web Single Sign-on. The centralized authentication relieves application programmers from identifying the user and it improves the user's convenience.</p> <p>The optional SMS login allows the usage of strong two factor authentication using the personal mobile phone as additional authentication token eliminating the effects of password phishing attacks. Existing legacy applications still relying on user name and password can be enhanced with this more secure authentication method without requiring any changes in the application.</p>
<b>A4</b>	<b>Cross Site Scripting (XSS) Flaws</b>	<p>The SES performs validation of all headers, cookies, query strings, form fields and hidden fields against a rigorous specification of what should be allowed. To further improve the reliability of script signature detection, the SES converts various character representations before verifying the content.</p>



<b>A5</b>	<b>Buffer Overflows</b>	<p>By working as a proxy and shielding the web server from direct access from the Internet, the SES significantly reduces the servers' vulnerability to attacks trying to exploit buffer overflows.</p> <p>Appropriate size checking on all such inputs can be customized for every web application using the form and parameter verification filters provided by the Secure Entry Server®.</p>
<b>A6</b>	<b>Injection Flaws</b>	<p>The elimination of injection flaws must be done on the affected web application. However, not all vendors may be aware of such a problem in their application or provide a patch in adequate time.</p> <p>The input and output filters provided by the Secure Entry Server® reduces the exploitation risk of various injection attacks by either blocking user input that contains commands used in injection attacks or by preventing to forward some web server output to the malicious client.</p>
<b>A7</b>	<b>Improper Error Handling</b>	<p>Although the Secure Entry Server® cannot prevent buggy web applications to crash or reveal implementation details that can provide hackers with important clues on potential flaws of the site, the Secure Entry Server® makes it difficult to exploit these flaws.</p> <p>Additional features such as load-balancing and fail-over further limit the impact of attacks for regular users.</p>
<b>A8</b>	<b>Insecure Storage</b>	<p>The Secure Entry Server® enforces a physical separation of the Internet, application servers and database network segments. Only HTTP/HTTPS requests are forwarded between Internet and the web application segment. Attackers cannot directly access information stored on servers behind the SES.</p>
<b>A9</b>	<b>Denial of Service</b>	<p>Web applications can't easily tell the difference between an attack and ordinary traffic. The SES includes different heuristics to detect Denial of Service (DoS) attacks and to minimize their effect. Minimal resources are used and available for unauthenticated sessions. Idle sessions or sessions not behaving as expected are dropped. Thus, DoS attacks will not be able to crash the SES or annoy authenticated users</p>
<b>A10</b>	<b>Insecure Configuration Management</b>	<p>The SES allows consolidation of the DMZ by enforcing centralized authentication, authorization, auditing and HTTP/HTTPS traffic inspection. This eliminates the problems with separate user management and access control for every web application. The additional line of defence imposed by the SES reduces both, the danger and the impact of misconfigurations and unpatched application servers.</p>



## Knowing/recognizing the user

All web applications are based on the HTTP-protocol, a stateless protocol used to exchange data between client and server. There is no mechanism to retain customer or provider identity and authenticity from one request to the next. This problem has been addressed in different ways. Unfortunately, many proposed solutions did not pay enough attention to security aspects.

Many attacks aim at taking over the identity or authorization of legitimate users (broken authorization, e.g. by cookie poisoning). If a hacker succeeds in taking over the identity of an authorized user, the possibilities for an automated defense are dramatically reduced. The more relevant a system, the greater is the danger of such targeted attacks. Not only current offerings but also information from management information systems are of huge financial interest to competitors or investors. In particular, such interests can include long-term, recurring and concrete financial and/or career-influencing goals of individual people. Like conventional industrial spying, successful attacks of this kind are difficult to prove, and are frequently only recognized or even suspected months or even years later. Known examples are attacks on hotels by competitors to gain unfair advantages for international invitations to tender. For business-relevant web applications, it is therefore of utmost importance for a WAF to provide penetration-proof authentication and authorization mechanisms.

The Secure Entry Server<sup>®</sup> offers several identification methods of various strengths. It even goes one step further and combines them with application access policies. The policy defines the requirements a user must fulfill before he/she can access a specific application. A user who authenticated using a weak method will simply not have the possibility to access systems containing sensitive data. Possible application security loopholes that allow more access than planned to a lesser privileged user are thus irrelevant. On the other hand, users with access to company-critical information need to be clearly identified by high-level authentication. A task that can be accomplished more easily upstream. Thus, illegal access to secure applications by non-authorized persons is already precluded at the system level.

The Secure Entry Server<sup>®</sup> by United Security Providers offers different authentication connectors for RADIUS, LDAP, SecurID (ACE Servers), Kerberos/NTLM and certificate-based login in PKI environments.

### Improper Error Handling

In WebSphere V6, users may see excessive instances of the following messages in Job Outputs:

```
Trace: ...  
ThreadId: ...  
FunctionName: ...  
SourceId: ...  
Category: ...  
ExtendedMessage: ...  
current Date: ...
```

This happens in the Deployment Manager and Node Agent Job Outputs. However they may also appear in the App Servers Job Outputs as well.

IBM, PK20802  
September 05, 2006



## Better performance and higher availability

As a general rule, increased security also means higher availability. The Secure Entry Server<sup>®</sup> furnishes proof of this statement. The people responsible for the system on the application computers experience the biggest advantage.

Defence against unauthorized access reduces the load on application servers as well as the environment's complexity, e.g. in the area of user management. In turn, both directly increase availability. Further, the SES serves as a load balancer between different application servers. Inquiries from the web are distributed amongst several servers and, consequently, each individual server's load is alleviated. Thus the SES can, unseen by the end-users, simultaneously cope with failures of individual back-end systems and take over the corresponding monitoring of escalation management of the back-end system. As a result, end-user experience is improved, contrary to the generally held notion that "security" equals "user-unfriendliness".

## Solution for the patch dilemma

The Secure Entry Server<sup>®</sup> limits the effects of vulnerabilities by providing extensible signatures which can be tailored to prevent the exploit of a security bug. By having the SES installed in front of your web applications and shielding them from direct Internet access, you can ease your web application patch policy.

Through the SES's upstream security controls, application computers become more serviceable vis-à-vis the Internet and less sensitive to security loopholes. Time-critical components of most security updates on application computers become irrelevant. Even for complex applications, the ability to schedule security updates for regular maintenance windows is an advantage directly resulting in operating and financial savings.

While the applications enjoy several advantages, the SES itself takes the brunt of the attacks and must be secured accordingly. In recognition of its importance, United Security Providers also offers services with patch notification or complete patch management (managed service).

## Tamper proven protection

As bastion host the SES is the first addressable component from the Internet - which is very likely to be attacked. The most important security measures to counter this are hardening the operating system and stripping-down the application in different modules, each running with the lowest privileges required to execute its tasks.

The Secure Entry Server<sup>®</sup> by United Security Providers uses a B1 certifiable security level, a TCSEC standard which is a

### Injection flaw

HP OpenView Storage Data Protector uses a proprietary protocol to communicate between the central backup server (Cell Manager) and backup agents.

By manipulating certain fields in the proprietary protocol, it is possible to pass commands to the backup agents even without being authenticated first. Any command can be sent and executed with the same privileges as that of the program.

NISCC Vulnerability  
Advisory  
August 29, 2006



comparable level to EAL 4 (Common Criteria) or E3 (ITSEC). Due to these preventions, the SES has never been hacked since its introduction in 1999.

Being shielded by the SES, your applications do not need to be on the same B1 level. This is very important as B1 security is very costly and hard to maintain since a B1 rated system enforces mandatory access control on operating system level. The system is divided into several compartments where it is not possible for program code running within one compartment to access resources within another compartment. Also, a separate administrator has to be configured for each compartment. By installing the SES in front of your existing applications, you benefit from the high level security without adding the administration hassle to each of your systems.

The SES enforces strong encryption (i.e. 1024 bit asymmetric key length, 128 bit symmetric key length) of the user session. To enhance performance, a hardware security module (HSM) can be installed to take care of the cryptographic algorithms and to provide secure storage for the web server credentials.

**Insecure storage**

Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies.

Apache Tomcat can be forced to reveal a complete directory listing for any directory by requesting a mapped file extension prepended with a semicolon, a reserved character. The file does not need to exist.

ScanAlert Security  
Advisory  
July 21, 2006

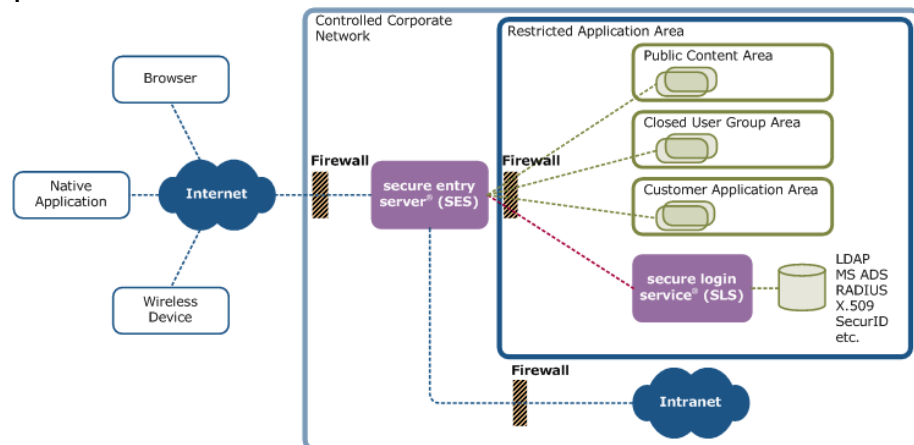


Figure 5: The Secure Entry Server® (SES)



## Use cases

In addition to securing your web applications and protecting your data from being eavesdropped, the Secure Entry Server<sup>®</sup> by United Security Providers offers many advantages for different business purposes.

The following examples illustrate some of the types of applications covered by the SES:

### Mail access for field workers

Mails typically contain sensitive data or confidential attachments. There is no way to get control or limit items accessed through web mail front ends without restricting its usability. Additionally, the user identification mechanisms offered are not adequate to the information exposed by mail proxies.

The Secure Entry Server<sup>®</sup> offers both data encryption to protect your valuable e-mails from being intercepted by curious competitors and optional enhancement of user authentication up to secure two-factor authentication.

### ERP connection for remote agencies

Distributed enterprises always encounter a trade-off between keeping data consolidated in the head office or offering redundant information in different branch offices. More and more ERP systems move to web-based technologies to solve the problem. The data is kept in the head office and branches access live data with browser-based clients. While this solves the problem of distributed data it is also a honey pot for everyone interested in your customer or HR database.

The Secure Entry Server<sup>®</sup> by United Security Providers knows the techniques attackers use to get access to your data and efficiently blocks all data thefts and manipulations. It has specific configurations for the major ERP systems and can be installed as a managed service that does not require any knowledge and monitoring from the user.

### Shield your valuable web applications

A broad variety of available web and application servers already offer valuable services for many companies. While the functionality of the applications may still be satisfactory, the applications may be vulnerable to new kind of attacks evolved over the time of their existence.



The Secure Entry Server® effectively blocks all kind of attacks executed on web servers and web applications without requiring any changes in the existing applications.

## User authentication for sensitive data

Some applications might still use weak username and password user authentication while newer ones already work with certificate based authentication. How can you ensure the same level of user identification for all you web applications without hiring a bunch of programmers updating your code?

The Secure Entry Server® consolidates the login process to one single identification step executed during your first request of a web application. The authentication method used can be a completely different and on a much higher security level than the one requested by your applications. Thus with the simple installation of the SES you enhance the authentication of all your existing applications.

## Re-Authentication for critical transactions

While implementing e-banking or other e-commerce solutions, there is only one effective way of securing critical transactions from being executed from malicious users that might have managed to sneak the legitimate user's password (phishing) or copy his strike list: Asking for a re-authentication based on a hardware token the will notice when it gets stolen.

The Secure Entry Server® by United Security Providers offers a toolkit for easy extension of existing applications to a multi factor authentication e.g. based on an RSA SecurID token or even on the users mobile phone. Assuming the user will lock it's mobile phone as soon as it's "lost", no attacker can authenticate on behalf of the user.

## Single Sign-on for portals

Employees typically use various applications to fulfil their tasks. Critical applications require user authentication. Handling these user accounts and the access rights gets a pain for both, the users requested to enter a password or other identification information for each application and also for the administrator suffering from the management of access rights and authorization changes.

The Secure Entry Server® features Single Sign-on for all web applications allowing the user to browse through different applications without the need to enter new credentials. The SES supports different authorization back-ends allowing the administrator to use his favourite IAM system to manage users and access rights also for web based access.



## Wiki or blog communities

The Internet is a perfect platform to share knowledge between experts and facilitate access to this information for others. Different companies offer forums, wikis, blogs or other means for employees to upload and share their knowledge. Again, these systems are vulnerable to attacks, specifically if documents and applications may be transferred from the Internet into the knowledge database.

The Secure Entry Server<sup>®</sup> by United Security Providers filters all data uploaded from the Internet to your web servers and allows to further verify documents and applications e.g. for viruses and malicious code. This feature can easily be added also to already existing systems without interfering with the already established community processes.

## Web Services

Providing machine usable web services is the next step in the evolution of web applications. Enterprises may package some of the functionality provided by their applications in services accessible by remote systems over the Internet. These web services may not only be used by branches and subsidiaries but also sold to customers and partners.

The Secure Entry Server<sup>®</sup> verifies all requests for web services and is able to ensure authentication and accounting for some or all of your services offered on the Internet. The SES guards the input and checks the content of all SOAP and XML messages used in web services.

## Online questionnaires

More and more processes are automated and accessible through the Internet. Process execution often requires entering data in online questionnaires or forms. Consider an insurance agent filling out a loss form. Some data he needs to enter must be detailed and verbose. In some cases he might run into a timeout on the web application and might lose all information he entered in the system.

The Secure Entry Server<sup>®</sup> by United Security Providers offers a special data cache for form data. Even if the insurance agent runs into a timeout, the data will transparently be reposted after the user has been reconnected to the system. Needless to say, that privacy and secrecy are also important features provided by the SES.



## Conclusion

Only specialized and full fledged web application firewalls efficiently protect your infrastructure from cyber attacks and malicious users. The Internet does not sleep and servers are probed in regular intervals for known vulnerabilities. Systems exposed to the Internet need to be hardened and regularly patched and monitored. If you do not have the time or expertise to patch and monitor your systems, consider using an appliance providing 7/24 managed services. However, protecting your servers is an important but not the only aspect of web application security. Keeping the list of users up to date and enforcing a careful and secure user authentication is a second piece of the overall security. The selected solution must also impede attackers from taking over the identity of legitimate users, e.g. by stealing some session information. There are many concepts to hold and delegate user identities. A good web application firewall supports all major concepts of session handling and offers different options to bind session and authentication information to a specific user and accordingly verify that he has not been tricked.

One aspect often neglected during the evaluation of web security is the ease of integration and operational excellence offered by the tools. A web application firewall cannot be installed and left alone. All new applications need to be integrated in the security infrastructure and operational tasks on the application gateway may effect the availability of your web applications. A considerable part of the costs accumulate in this phase and systems not optimized for integration might turn out to restrict your degree of freedom in an unacceptable way.

The Secure Entry Server<sup>®</sup> has proven its flexibility and reliability day-to-day in many installations worldwide enabling our customers to run and maintain their business critical applications. Many of its operational features are based on our long experience and tight collaboration with system and support engineers. Its flexibility is not limited to the different authentication methods, ease of application integration and support for many IAM back-ends but also includes attachment to various logging, monitoring and alarming systems, system management tools, anti virus providers and deployment mechanisms.

For companies that do not have free resources to monitor and update the security infrastructure United Security Providers together with its partners offers a flexible range of managed security services. You get a well protected system supervised 7/24 by security experts at calculable costs.