Intelliwall

Présentation OSSIR - 14/09/2004

Nicolas Dirand Directeur R&D ndirand@bee-ware.net
Eric Battistoni C.T.O. ebattistoni@bee-ware.net

Web Application Gateway
Introducing Bee Ware

History
- Founded in November 2003 by Nicolas Dirand, Creator of Qualys and Christophe Guyard, Former President of Axians, one the Largest French Network and Security Integrators.
- Headquartered in Paris with R&D facilities in Aix en Provence
- International Headquarters in Brussels.

Strong Business Model
- Technology Innovation
- Strong Channel Partnership
- Technological Partnership

Mission
- Secure Web-Based applications by a tailored and comprehensive Firewall Web Application Technology protecting Web-sites from known and unknown attacks.

Customers
- Among the Fortune 1000 customers, Bee Ware has won major references in the Finance, E-Business and Transportation Industries.
Web services are the leading technology for value added services.

HTTP is one of the only protocols allowed to pass through the internet firewalls.

Web applications rely on many languages, scripts, libraries... there are infinite possibilities for discovering vulnerabilities.

Deploying Internet, Intranet or Extranet technologies is a Business Enabler.

Firewall and Intrusion Prevention Products efficiently protect the network and system layers through centralized access control mechanisms.

Customers’ data, market and finance figures, and a lot of confidential information are within reach for malicious users.
Application attacks are real life

The Web components have not been designed with security concerns in mind.

The existence of an application attack often remains unrevealed.

Web technologies are popular and affordable. Publishing or manipulating information becomes quite easy, for both programmers and hackers.
Network
Attacks target the protocol level: IP Spoofing, TCP-Based Attacks...
Firewalls and strong authentication are the most common answer, providing access control security.

System
Systems are typically targeted using openly disclosed vulnerabilities (such as they are found in MSRPC, IIS, Cisco IOS and many other systems etc).
Secured by intrusion detection, monitoring, patch management.

Web
HTTP is a connectionless, open and permissive protocol. Securing Web servers is not only about HTTP. Web applications also include HTTPS, PHP, CGI, Perl, XML, SOAP...
Hackers already know that existing security infrastructures are unable to understand Applicative queries. None of these security solutions can pit effectively against attacks at the application layer.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Malicious requests detection</td>
</tr>
<tr>
<td>System</td>
<td>Vulnerabilities prevention</td>
</tr>
<tr>
<td>Network</td>
<td>Identity checking and protocol filtering</td>
</tr>
</tbody>
</table>

Filtering on the action intention for application access control.
Understanding the application diversity,

The application layer:
A multi component layer.

User’s developments
Languages & Scripts
Applications Servers
Web Servers
Operating systems
Application services
Application Layer – OSI model
...to figure out the risks.

Potential for application vulnerabilities is endless

Differences of:
- Conception
- Parameters
- Libraries
- Languages
- Systems
- Protocols

Volume of parameters to address
Diversity is Endless.

Is determinism...
Applied on Web security, still a quality criteria?

Adapted to low layers...
These areas can be considered as identified and under control.

Relevant for an unknown perimeter...
The potential of vulnerabilities is boundless

Constraints are more and more increasing
Knowing ALL that’s forbidden, ALL that’s authorized, and knowing it ALL the time ??
## Top Ten Vulnerabilities

**2004 update**

<table>
<thead>
<tr>
<th></th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Unvalidated Input</td>
</tr>
<tr>
<td>A2</td>
<td>Broken Access Control</td>
</tr>
<tr>
<td>A3</td>
<td>Broken Authentication &amp; Session Mngt</td>
</tr>
<tr>
<td>A4</td>
<td>Cross Site Scripting Flaws</td>
</tr>
<tr>
<td>A5</td>
<td>Buffer Overflows</td>
</tr>
<tr>
<td>A6</td>
<td>Injection Flaws</td>
</tr>
<tr>
<td>A7</td>
<td>Improper Error Handling</td>
</tr>
<tr>
<td>A8</td>
<td>Insecure Storage</td>
</tr>
<tr>
<td>A9</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>A10</td>
<td>Insecure Configuration Management</td>
</tr>
</tbody>
</table>
Network-layer security mechanisms dominate current deployments but are proving inadequate in the face of more frequent application layer attacks.

META Group

Application Gateways will become the darling of enterprise security architectures.
Firewall devices from Cisco, Check Point, Netscreen and Symantec will enforce the protocol structure but will need to be backed up by layer 4-7 inline application gateways to enforce application business logic.

Yankee Group – 2004 Predictions

Rethinking IDS
“Aside from IPS, another category to consider for specifically protecting Web servers and other DMZ applications is a Web application firewall.”

CSO online 03/2004

Today over 70% of attacks against a company’s network come at the « Application Layer », not the Network or System Layer.

Gartner Group

Forget about patches
Researchers at the Florida Institute of Technology are looking for ways to fight hackers by modeling their methods, or “exploits.” The research could eventually lead to new types of security tools capable of stopping attacks that hackers haven’t even invented yet.

Computerworld March 2004
Marketing
The current traditional security players have to preserve their market shares...Whether they have a solution or not.

Technology
How should the web application security problem be addressed?
With a solution based on: Traditional security concepts...a current technology enhancement...or an innovative concept?

User satisfaction
How to fill the security gap, with accuracy but without increasing additional administration tasks overload.

!!! Customers have been warned by the bad IDS experience !!!

by BeeWare
Many technologies and solutions pretend to secure the application level. And that’s partly true.

But considering the accuracy, the performance, the management tasks... the gap between security needs and reality becomes a growing issue.

Reverse Proxy alternative: poor level performance, time consuming and inappropriate configuration tasks.

Deeper inspection: secured, but partial inspection. High expertise required for the security administrators.

New approaches: Intelligence
Proxy and Reverse Proxy

How does it work?

Is a proxy an application security device?

Once upon a time, at the early ages of security...
HTTP Proxy isn’t Web Proxy

A true Web Reverse Proxy should involve not only an HTTP proxy, but an SQL proxy & PHP, CGI, PERL proxies as well...

The Proxy concept is slow (Client & server emulation).

There can easily be breaches in the components or implementation of a Proxy.

Proxy architecture is poor in performance
An HTTP Reverse Proxy has to rely on others mechanisms in order to provide an in depth application analysis.

In the Reverse Proxy model, the application security is achieved by a very basic White List concept.

Key question is: Which is the best technology to protect the application?
The White List approach

It’s a very basic & simple concept...

but which introduce a much more complex issue:

Despite the help of discovery tools, a White List approach is a complex process (to develop, maintain and exploit) which should be cautiously evaluated before being deployed.

White List security only rely on user’s efforts
Product Introduction
“According to a recent survey from the Cambridge University, how the letters are arranged within a word hasn’t a big importance. The human brain isn’t based on such linear reading. Picking up the most relevant signs is enough, and quicker, to show us the meaning of the whole word and sentence.”
Intelliwall mimics the human approach, using its analysis and its expertise.

The neural network technology, already used in some applications like character recognition, content filtering or financial assessments, provides a “fault tolerant” reading of the traffic.
One of the main strengths of Intelliwall’s neural kernel is its capability to detect the "intention" of a query through the instant interpretation of evidences.

The efficiency of our solution does not only rely on neural networks but on the way we adapted this technology to meet Security needs and culture. The intelligence comes from the recognition skill (position of the sensors) and training capabilities.
Intelligence based on training

Pre-training + on-site training
- 0 False positives

Regular Traffic
- Approved requests
- Forbidden requests

Attacks & malicious traffic

Intelliwall

by BeeWare
Web site access profile

A **User black list policy** prevents any hacker from proceeding to a step by step analysis of the site.

**Profiling the Web Site**

The profiling feature is based on the powerful RegExp expression model.

This provides the ability to restrict access to the dev or back-up folders of the site.
Application security policy

Any security solution needs to allow a customer policy customization in order to be accurate and effective.

**Applicative security policy** deals with protocol but with languages as well.

**System security policy** includes both authentication, open services, and vulnerabilities prevention.

**Network security policy** is based on identity, origin and destination, protocols and ports.
Intelliwall client is based on Java. It can run on any platform supporting Java (Windows, Unix, Linux, Mac...)

Configuration and set up are just a few clicks. In just a few minutes, Intelliwall footprints the traffic and is ready to proceed.

The Intelliwall client installer is very simple to run. Java run-time is included and auto-installed (if needed).
Intelliwall G.U.I.

- Real time traffic monitoring
- Train Brain
- Brain back-up
- Exclusions
- Reporting
- Real time monitoring features
- Logs and reports

**Monitoring:**
- Graphic User Interface
- SMTP Trap alarms
- MAIL SMTP alarms

**Reporting:**
- Syslog client
- Logs export XML format
- Logs export CSV format
- Printable reports (PDF) with scheduler
Training steps

- Select the legitimate queries
- Click on the Train button
- A train progress window will keep the administrator updated
Serial or parallel connection

Easy to plug-in any architecture

Serial connection « in-line mode »

Parallel connection – « sniffer mode »

Management Interface
SSL architectures

HTTPS support

In case of no SSL accelerator

In case of SSL accelerator

IntelliWall in SSL Mode
Reads encrypted files

IntelliWall in normal mode
Analyzes decrypted flows

by BeeWare
Heavy and repetitive tasks make a security product impossible to manage and unable to perform its goal.

Intelliwall management tasks are “light”:

- **Configuration**
  - Address setting
  - Alarms setting

- **Monitoring**
  - Exclusions adjustment
  - Brain train (close to 0 after a couple of days)

- **Updates**
  - Minor releases & patches (automated)
  - Major releases

**Fast and efficient.**

Such as the dialog between two experts.
Product Summary

Intelliwall
Reverse Proxy
Correlation
Deep Inspection
Intelliwall is Easy to Try

- Non disruptive. Intelliwall is plugged in passive mode and just listen to the traffic.
- No configuration. Just a few parameters regarding the Web server to be protected.
- Immediate result. Just after being plugged in front of a Web site, Intelliwall starts working and detects all the suspicious requests.
- Proof of concept. Using the Training facility, customers will be able to reach the 0 Falses Positives challenge in a couple of days.

How to subscribe?

- An Intelliwall “Try” is just one week long, it’s easy to plan and will not be time consuming.
- Identify a Web application to be monitored by Intelliwall with a significant traffic.
- Involve the application developers, or ask for the Bee Ware support, in order to look at the application structure, and to demonstrate how Intelliwall secures the application.
- A report will be made following the “Try”, including comments about the traffic, the potential breaches, and the Intelliwall response.