WAPPLES | White Paper

WAPPLES

Intelligent Web Application Security

Penta SECURITY

In the interconnected world of today, businesses depend on information technology systems not merely to store data, but to interact with clients and employees, and to offer products and services to their customers. The vast increase in web applications over the past two decades has turned the internet into a dynamic global environment of commerce and communication. Unfortunately, while businesses have expanded their global reach via the web, they have also exposed themselves to far greater risk. 'Information Security' once meant simply a locked safe inside an office; however, the thieves of today need not employ a set of lock-picks. In fact, the most skilled thefts of today can be committed without the thief so much as leaving his desk – yet these attacks can cause severe harm to the victim, ranging from theft of proprietary or private information, to the loss of funds or clientele. Modern security extends far beyond the simple notion of lock and key to include network and information technology security experts, as well as security hardware and software. However, as the virtual environment continues to evolve, those who seek to exploit web application vulnerabilities continuously devise new methods to bypass existing security measures.

Information Security staff – the security guards of the virtual world – have struggled to keep pace with the ever evolving skills of hackers. When virtual networks were in their infancy, they were a constant focus of both hackers and security specialists alike. As networks grew more mature, their security systems matured as well. However, while many organizations have remained focused on network security, the hacking community has turned its attention to something more vulnerable: the web application layer. Located outside of the now ubiquitous network firewall, web applications are often unprotected and highly vulnerable to attacks.

Once web applications became the number-one target of hackers, a new form of security was needed to protect the virtual environment. Web application firewalls (WAFs) were introduced by a variety of information technology security firms for the purpose of defending web applications against the rapidly growing arsenal of threats that they faced. Unfortunately, the shortcomings of the early generations of WAFs, such as their cost, labor intensiveness, lag time during installation, and high rates of false positives discouraged many organizations from utilizing WAFs to protect their systems. Due in part to the drawbacks of the original WAFs, many businesses clung to the mistaken belief that pre-existing network security systems would be sufficient – a choice which has led to the loss of personal and proprietary information, funds, and customer trust from a wide range of businesses across the globe.

In response to the need for an affordable, easy-to-use, and reliable web application security product, WAPPLES – the latest generation WAF from Penta Security Systems, Inc. – was created. WAPPLES offers cost-effective, minimally labor intensive, and highly accurate web application security, powered by an intelligent, logic-based engine, capable of keeping pace with the rapidly evolving threats which target web applications.

Hackers in the Headlines

Hackers made the headlines throughout 2011 as international companies, financial institutions, and government agencies fell victim to devastating hacks.

- In early 2011, representatives of the NASDAQ stock exchange announced that in late 2010 their custom web application, Directors Desk – an application used by all companies traded on the exchange – had been breached, allowing hackers access to a wealth of confidential and proprietary information.[1]

- In June 2011, the well-known hacker group, LulzSec announced that they had penetrated Sony's virtual records by means of a SQL Injection attack. LulzSec claimed to have stolen the records of more than one million Sony customers, although Sony claimed that just under 40,000 records had been accessed. No matter the specific number of records leaked, the fact remains that recovering from the loss of customer trust and business caused by this attack will be difficult for Sony.[2]

- In June 2011, LulzSec made the headlines again when it disabled the official website of the Central Intelligence Agency (CIA) of the United States of America for a period of several hours.[3]

- In July 2011, the Deputy Secretary of Defense of the United States announced that earlier in the year the Pentagon had been hacked, resulting in the loss of 24,000 files, although the Pentagon has not released the method by which this hack was accomplished.[4]

Government Hacked: 24,000 Files Stolen in Worst Pentagon Cyber Attack

July 14, 2011 4:19 PM EDT

America's defense agency is having trouble defending itself, as th Pentagon lent a sense of urgency to the institution's push to s by bolstering cyber security.

Sony hack: private details of million people posted online

Hackers have attacked Sony and stolen the private details of more than a million people in the latest security breach to hit the electronics giant.

By Andy Bloxham 7:51AM BST 03 Jun 2011

The names, birth dates, addresses, emails, phor passwords of people who had entered contests p all published on the internet

LulzSec, a hacker group, said it had infiltrated the firm's syst prove how vulnerable they were to "simple attacks".

Nasdaq hackers gathered listed companies' secrets

Jim Finkle October 21, 2011

Hackers used the stock exchange's DirectorDesk app to spy on others.

Trading activity is displayed on electronic boards at the Nasdaq Marketsite in New York in March. Its systems were hacked in February. Photo: Jin Lee

Some of the most well-known hacking victims of 2011included the US Government, Sony, and NASDAQ.

Got an App for Risk?

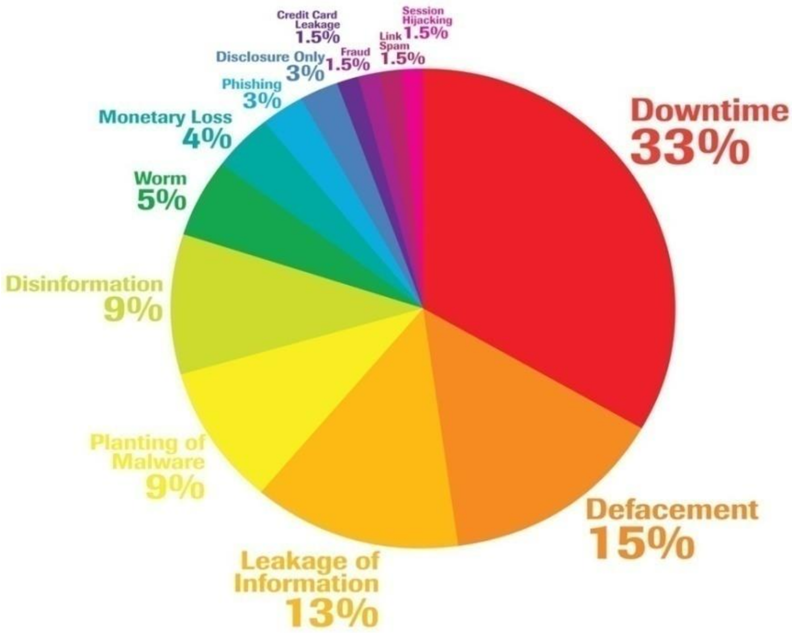
What is a web application? A simple definition provided by CGISecurity is "a multi-layered entity that includes code and data residing in many places within the enterprise that can be accessed directly or indirectly from the Internet."[5] Thanks to the late Steve Jobs, the phrase *'There's an app for that'* has entered the modern lexicon, and web applications have proliferated at an exponential rate. Yet while web applications flourish, they remain vulnerable to a wide range of threats.

According to the well known information technology research firm Gartner, Inc., in recent years hackers have focused roughly 75% of their attacks on web applications. According to an analysis of over 12,000 websites conducted by the Web Application Security Consortium in 2008, the most common web application vulnerabilities were HTTP response splitting, SQL injection, information leakage, and cross site scripting (XSS).[6] More recent reports show that these threats are not going away.

The Open Web Application Security Project (OWASP) released a report entitled OWASP Top 10 – 2010, which outlined the ten most critical web application security risks of 2010. According to OWASP, the top ten web application risks are as follows: Injection (including SQL, OS, and LDAP), XSS, Broken Authentication and Session Management, Insecure Direct Object References, CSRF, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, and Unvalidated Redirects and Forwards.

Researchers from the Ponemon Institute surveyed 637 information technology and security professionals from a variety of industries regarding their companies' web application security practices. The results of the survey were released in February 2011 in a report entitled State of Web Application Security – and it contained surprising results. According to the Ponemon report, 73% of the organizations surveyed admitted that they had been hacked within the past two years, yet 72% admitted that they hadn't tested 90% or more of their web applications for vulnerabilities. Additionally, the Ponemon report stated that "Network firewalls are the most popular method used to augment and secure web applications, which shows a severe lack of knowledge about web application security." As network firewalls are designed to provide security protection to the OSI Layer 3, the network layer, they cannot provide adequate protection to the OSI Layer 7, the web application layer

The results of relying only upon network firewalls for web application security can be devastating. According to Trustwave's Web Hacking Incident Database report for the second half of 2010, the results were severe indeed. 33% of hacking incidents resulted in web application downtime, meaning an inability to successfully conduct business, or to communicate with and serve customers. 15% of hacking incidents resulted in website defacement, causing businesses to display incorrect or even offensive information on their websites. 13% of attacks led to leakage of information – an event which can be detrimental to a business on a variety of levels, ranging from loss of customer trust and service, to theft of proprietary information.

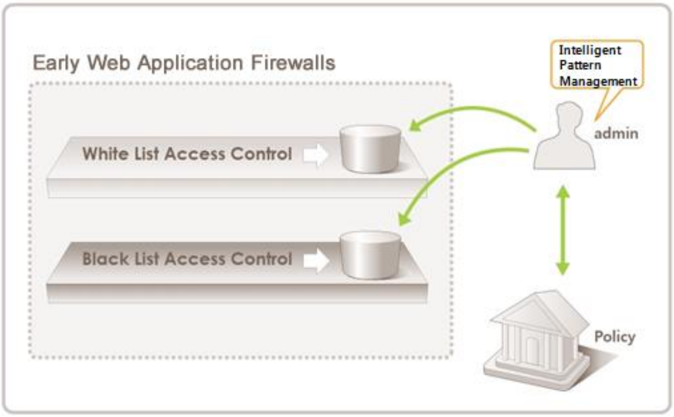


Graph courtesy of Trustwave's Web Hacking Incidents Database report for the second half of 2010

Given the risks resulting from weaknesses in the web application layer, the Verizon 2011 Data Breach Investigation report makes an excellent point: ***"It is no secret that attackers are moving up the stack and targeting the application layer. Why don't our defenses follow suit?"*** The threats to web applications are clear. Yet why have so many large businesses been reluctant to install web application firewalls, products specifically designed to protect web applications? The answer can be found in the flaws inherent in previous generations of WAFs.

Drawbacks of Previous WAFs

The major operating principle of **first generation WAFs** was pattern matching, a process that involved extensive administrative manpower. After an administrator added a known attack pattern (black list), the first generation WAF compared web traffic to the updated patterns by analyzing them at the application level. Unfortunately, with the first generation WAF there was no detection system for new or modified attacks. Additionally, attempts to add patterns for all conceivable attacks led to both a deterioration in web application performance, an increase in false positives, and a heavy workload for the WAF administrative team. The high costs of manpower required to operate a first generation WAF, combined with its inability to protect against new or modified attacks, its tendency to produce false positives, and its poor system performance limited its success in the IT security market.


Early Web Application Firewalls
Intelligent Pattern Management
admin
White List Access Control
Black List Access Control
Policy

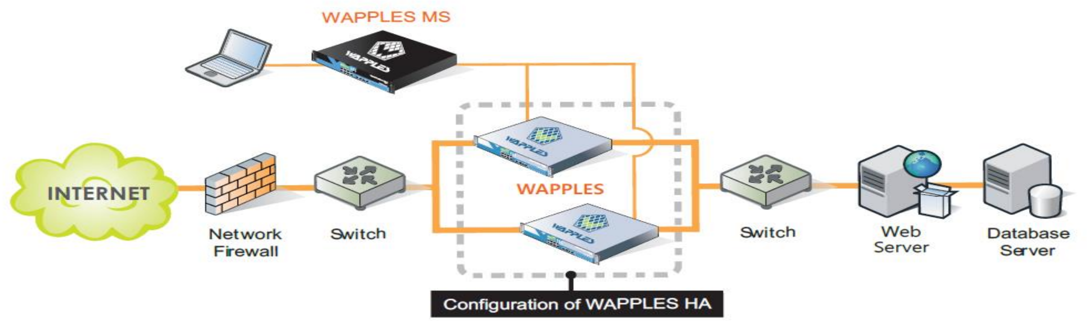
The **second generation WAF** attempted to remedy the flaws and limitations of the first generation. By analyzing the web application(s) protected by the WAF, the second generation WAF was able to automatically establish a security policy (white list). Unfortunately, such automatically established policies could take up to two weeks to implement, rendering this solution impractical for the rapidly changing environment of the web. Additionally, while the policies were established automatically, they still required manual configuration by an administrator, thus increasing – not reducing – the administrative burden. Lastly, as pattern matching remained the basis for the second generation WAF, it still suffered from many of the limitations which afflicted the first generation WAF, namely an inability to protect against unknown attacks, a tendency to produce false positives, and slow system performance.

Meanwhile, the threats against web applications endured and evolved. The web application layer remained vulnerable and a frequent target of hackers. A solution was needed, one which could overcome the drawbacks of the early generations of WAFs to offer secure, reliable, cost-effective, and easy-to-use security. A new breed of WAF – an intelligent WAF – one based on an entirely new concept, was needed. Such an intelligent WAF would need to be capable of analyzing web traffic, detecting attacks, analyzing and classifying them, and finally, applying appropriate countermeasures to block detected attacks. An intelligent WAF would need to be able to perform these functions without the continual involvement of administrative staff, in order to protect web applications in a stable manner while easing the administrative workload and management costs.

WAPPLES: The Third Generation WAF

In response to the need for an intelligent WAF that could meet the both the security and administrative needs of the modern business world, Penta Security Systems, Inc. created **WAPPLES**: the **third generation WAF**. Unlike previous generations of WAFs, WAPPLES is equipped with an intelligent logic analysis engine, designed to identify attacks against the web application (whether previously known or unknown) and defend against them. The highly intuitive graphic user interface (GUI) enables the administrator to easily and conveniently establish a security policy – one which will not need to be altered even if the web application is modified, or if new attacks arise.

WAPPLES can be installed without changing the existing network system configuration, and it can be installed upon various network configurations, including in-line, reverse proxy, High Availability (HA), and more. Additionally, WAPPLES offers secure web application protection immediately upon installation, without the need for a lengthy profiling and learning period. The available suite of WAPPLES hardware appliances enables scalability and continued protection for a growing business with an expanding network. If needed, Penta Security Systems, Inc. offers WAPPLES MS, a centralized management system that allows for remote integrated management of groups of WAPPLES units, enabling streamlined management of large web application firewall systems.

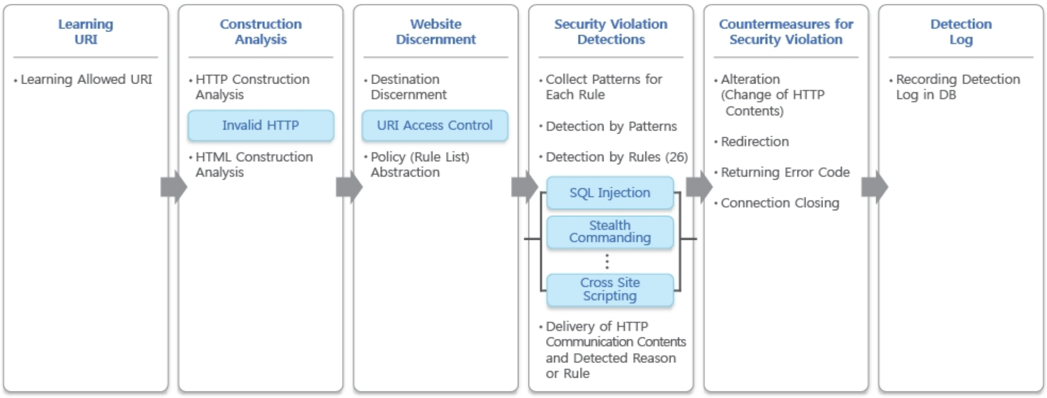


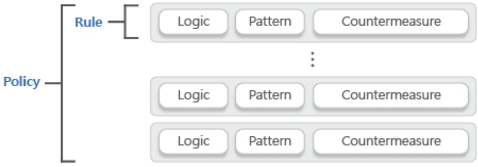
[Configuration Example of WAPPLES HA and WAPPLES MS “Management System”]

The COCEP Engine and its 26 Rules

WAPPLES runs on an intelligent logic analysis engine called Contents Classification and Evaluation Processing, or COCEP. This logic analysis engine utilizes a system of 26 ‘rules’ (see Appendix C for detailed explanations of each rule) to execute a logical analysis of all types of traffic. This analysis enables WAPPLES to determine whether or not the traffic constitutes a threat to the web application, and to take appropriate countermeasures when threats are detected. If traffic can successfully pass through all 26 rules, WAPPLES determines that the traffic is not an attack, and transports the data to the web application. The split-second performance of the COCEP enables WAPPLES to determine if traffic is safe in just 1/1000 of a second, leaving system performance unaffected.

Unlike previous generations of WAFs, WAPPLES does not require the administrator to add patterns manually, as the COCEP logically recognizes attacks (whether previously known or unknown) on its own. Likewise, the automated functionality of WAPPLES allows it to automatically respond to attacks detected by the COCEP, without involving administrative personnel. Additionally, as the COCEP engine operates on logic, rather than pattern matching, WAPPLES has been able to achieve a near-zero false positive rate. WAPPLES offers intelligent and accurate protection against threats that target web applications, enabling PCI-DSS certified security and the ability to detect and block the threats enumerated in the OWASP Top Ten – 2010 report. Web attack detection and response through the logic analysis of the COCEP have made WAPPLES the new paradigm of web application security.

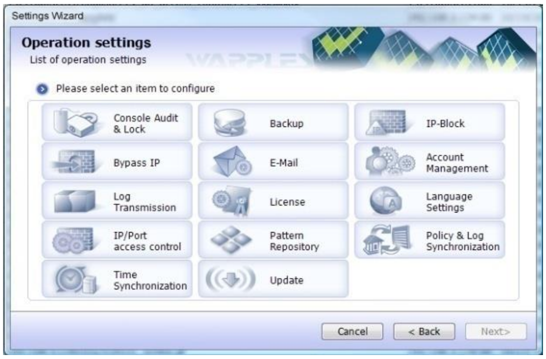

Learning URI
• Learning Allowed URI
Construction Analysis
• HTTP Construction Analysis
Invalid HTTP
• HTML Construction Analysis
Website Discernment
• Destination Discernment
URI Access Control
• Policy (Rule List) Abstraction
Security Violation Detections
• Collect Patterns for Each Rule
• Detection by Patterns
• Detection by Rules (26)
SQL Injection
Stealth Commanding
⋮
Cross Site Scripting
• Delivery of HTTP Communication Contents and Detected Reason or Rule
Countermeasures for Security Violation
• Alteration (Change of HTTP Contents)
• Redirection
• Returning Error Code
• Connection Closing
Detection Log
• Recording Detection Log in DB



* A conceptual diagram showing the operating principles of WAPPLES and its COCEP engine.

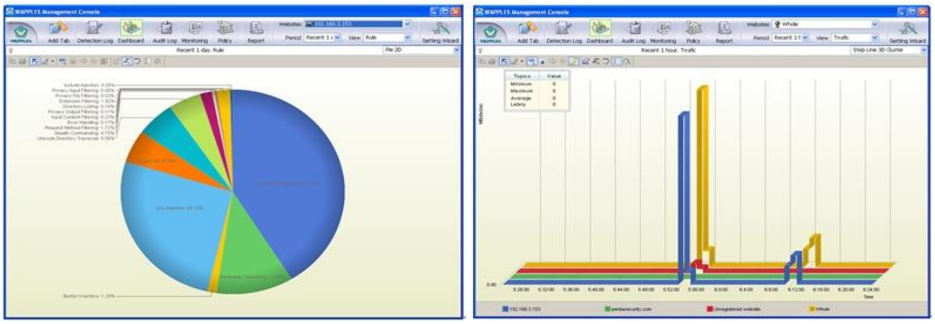
User-Intuitive GUI

WAPPLES boasts an easy-to-use and user-friendly GUI, which enables rapid policy configuration through the use of a simple settings wizard. It also offers real-time monitoring of attack detections and system status, as well as customizable reporting. The WAPPLES GUI is not only easy-to-use, but can be easily customized based on user-preferences, enabling convenient management and monitoring of the information which the user deems most important.



Settings Wizard

The monitoring function allows the administrator to view the top ten detection results recorded by WAPPLES during the most recent hour, and said results can be sorted by attack type, attacker information, and host information. The WAPPLES Dashboard displays charts which show traffic, as well as attack detection log information. The dashboard reanalyzes the detection log information every ten seconds, and updates the screen accordingly. Information that can be analyzed via the dashboard includes traffic, page hits, attack detection logs, distribution by rule, system status, network status, etc.



Sample graphs from the WAPPLES Dashboard

What differentiates WAPPLES from its competitors?

- Based on a new concept of web application firewall, WAPPLES resolved the fundamental problems of previous generations of WAFs.

- While the first and second generation WAFs could not deal with new or modified attacks on an immediate basis, WAPPLES can intelligently detect and block known, new, and modified attacks immediately by logically analyzing web traffic. The logical analysis method (as opposed to the pattern matching method employed by previous generations of WAFs) can reduce false positives to nearly zero.

- Highly skilled administrative staff are not required to operate WAPPLES, due to the combination of its easy-to-use GUI and the intelligent COCEP engine.

- As WAPPLES itself, not an administrator, is responsible for both detecting attacks as well as determining and launching appropriate countermeasures, the burden on administrative staff is minimal. This allows organizations to save money on administrative overhead while simultaneously enhancing the security of web applications and confidential data.

- WAPPLES provides security immediately upon installation, as a long profiling and learning period are not needed.

- Using WAPPLES, the security administrator can establish a customized security policy simply by determining whether or not to apply each rule, and if so, by setting the appropriate level of response. The established policy will not require modification if the web application is altered, or if a new type of attack is developed.

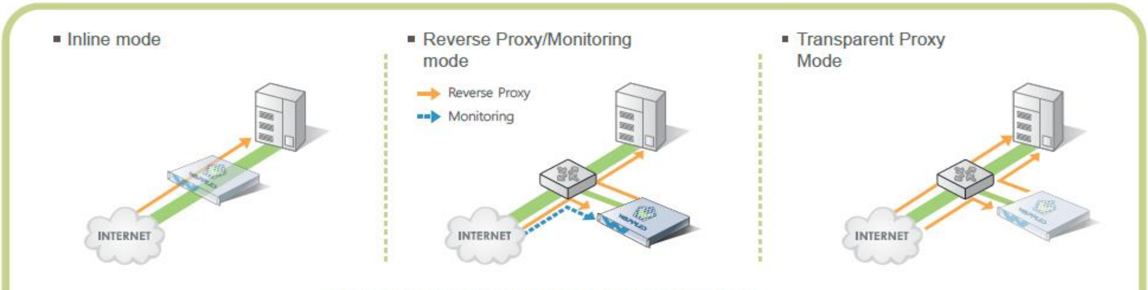
- WAPPLES offers a high level of performance, without regard to environmental influences, such as administrator capabilities or system configuration.

- WAPPLES creates detailed logs of threats detected and blocked, which can be customized by threat, origin, time period, etc.

- WAPPLES provides reliable and accurate protection against the ‘OWASP Top 10’ vulnerabilities, and enables PCI-DSS compliance.

- For large organizations with multiple WAPPLES units, WAPPLES MS is available to enable remote integrated management of groups of WAPPLES units.

- WAPPLES can be installed upon various network configurations, including in-line, reverse proxy, transparent proxy, and High Availability.



[Configuration Diagram for the Installed WAPPLES]

A WAPPLES Success Story: Aeon Mall

http://www.aeonmall.com

Aeon Mall Co., Ltd. is a well-known Japanese shopping mall developer. Established in 1911, the company has grown and expanded to an empire of shopping centers throughout Japan. Aeon Mall operates on a 'customer first' philosophy, and incorporates the needs of both customers and the community into all stages of shopping center development. The goal of Aeon Mall is to make their shopping center facilities indispensable parts of their respective communities.

Problems facing the Aeon Mall website:

- Attacks on the Aeon Mall website were initially dealt with by strengthening the security of its infrastructure, a solution which was proven to be unsuccessful.

- Costs of administration and maintenance of existing security measures were expensive, while the results were ineffective.

Problems facing the Aeon Mall website, continued:

- Aeon Mall found itself facing a sudden increase in attacks against their website.

- Aeon Mall experienced DoS/DDoS attacks which paralyzed network equipment, such as the router and network firewall.

- The Aeon Mall website itself was paralyzed, and their web service was stopped.

- The results obtained via a security vulnerability scan of the Aeon Mall website revealed that, due to attacks on the web application in the form of cross site scripting, the web server structure and website had been tampered with, phishing agents had gained access, and leakage of personal information had occurred.

Results of Installing WAPPLES

- With the installation of WAPPLES, the installation, administration, and maintenance costs of web application security have been reduced.

- Even when Aeon Mall web applications and website contents are modified, secure protection continues without the need to modify the security policy configurations.

- Through use of WAPPLES, Aeon Mall now complies with the Payment Card Industry Data Security Standard (PCI-DSS).

- Secure, stabilized web service is now provided together with strengthened infrastructure.

- Attacks against the Aeon Mall website, including DoS/DDoS, XSS, website defacement, and theft of personal information are now prevented.

- System administration and maintenance costs have been reduced, and undivided attention can now be paid to the original service goals of Aeon Mall.

WAPPLES: Intelligent Web Application Security

As the virtual environment evolves and expands, the threats against web applications continue to proliferate and grow ever stronger. Businesses that do not take proactive steps to secure their web applications risk system downtime, website defacement, leakage of private information, and much more, all of which can lead to loss of customer trust – and worse – loss of business. As hackers continue to focus their attention on the web application layer, businesses must defend themselves. While it is vital that organizations secure their web applications, it is also imperative that they do so in an efficient, accurate, and cost-effective manner. Previous generations of WAFs, while designed to defend the web application layer from attacks, were incapable of doing so efficiently, accurately, or cost-effectively. High rates of false positives, combined with slow system performance and extreme labor intensiveness discouraged many businesses from relying on WAF protection.

WAPPLES offers the intelligent solution to web application security, by providing a secure, reliable, and efficient method to protect web applications in a cost-effective manner. Utilizing its logic analysis based engine, WAPPLES intelligently detects and blocks both known and unknown attacks, allowing it to keep pace with the rapidly evolving threats of the virtual environment. Additionally, WAPPLES boasts a user-intuitive GUI that enables web application management to be performed by a small team, thus decreasing administrative costs while increasing both efficiency and security.

The threats facing web applications are ever-present and continuously evolving. The best method for securing web applications is an intelligent and ever vigilant sentinel, standing guard over the web application layer. WAPPLES, as an intelligent and accurate – yet cost effective and minimally labor intensive – next-generation web application firewall, provides such a defense. With over nine years in the web application firewall industry, and with over 900 satisfied customers in East Asia, WAPPLES offers a tested and proven solution to web application security.

Appendix A: Sources

[1] CNET News Report: NSA Joins NASDAQ Hack Probe, by Stephen Musil, March 30, 2011, retrieved October 28, 2011 from http://news.cnet.com/8301-1009_3-20048996-83.html

[2,3] LulzSec, retrieved October 28, 2011 from http://en.wikipedia.org/wiki/LulzSec

[4] Washington Post, 24,000 Pentagon files stolen in major cyber breach, official says, by Jason Ukman and Ellen Nakashima, July 14, 2011, retrieved October 28, 2011 from http://www.washingtonpost.com/blogs/checkpoint-washington/post/24000-pentagon-files-stolen-in-major-cyber-breach-official-says/2011/07/14/gIQAsaaVEI_blog.html

[5] Ethical Hacking Techniques to Audit and Secure Web-enabled Applications, by Sanctum, Inc., 2002, retrieved October 25, 2011 from http://www.cgisecurity.com/pen-test/Auditing-and-Securing-Web-Enabled-Applications.pdf

[6] Web Application Security Statistics, last edited by Sergey Gordeychik, February 2010, retrieved October 25, 2011 from http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics

APPENDIX B: WAPPLES International Patents and Certifications

- Payment Card Industry Data Security Standard (PCI-DSS) Certification
- Korea National Intelligence Service CC Evaluation (EAL4) Registration No. NISS-2049-2010
- United States Patent: Method of Detecting a Web Application Attack US Application No. 12/876,820
- China Patent: Method of Detecting a Web Application Attack Chinese Application No. 201010287262.2
- Japan Patent: Method of Detecting a Web Application Attack Patent No. 2012-014667
- Korea Patent: Method for Detecting a Web Application Attack Patent No. 10-2010-0064363
- Korea Patent: Method for Detecting a Web Attack Based on a Security Rule Patent No. 10-2009-0077410

APPENDIX C: WAPPLES Rules

Buffer Overflow	Blocks invalid requests causing buffer overflow attacks
Cookie Poisoning	Blocks the falsification of cookies containing authentication information
Cross Site Scripting	Blocks malicious script code having the possibility to be executed by the client
Directory Listing	Blocks the leakage of web sites' directory and files
Error Handling	Controls error messages so as to avoid exposure of information about web server, WAS, DBMS server, etc.
Extension Filtering	Blocks access of files which do not have permitted file extensions
File Upload	Blocks the upload of files which can be executed on the web server
Include Injection	Blocks the injection of untrustworthy files and external URIs
Input Content Filtering	Blocks or substitute words that are not permitted on a web site
Invalid HTTP	Blocks access not in compliance with HTTP standards
Invalid URI	Blocks access not in compliance with standard URI syntax
IP Black List	Blocks when more than the set value of access attempts from the same source IP are detected during a specific time (value set by user)
IP Filtering	Blocks access to a specific IP range or countries (set by user)
Parameter Tampering	Blocks attacks which send maliciously manipulated parameters to websites
Privacy File Filtering	Blocks leakage of private information from files transmitted from the web server
Privacy Input Filtering	Blocks leakage of private information via HTTP request
Privacy Output Filtering	Blocks leakage of private information via HTTP response
Request Header Filtering	Blocks HTTP requests having headers that are missing important information or that have been abnormally modified, such as requests from automatic attack tools and abnormal HTTP requests

Request Method Filtering	Blocks risky HTTP request methods
Response Header Filtering	Blocks leakage of web server information via HTTP response
SQL Injection	Blocks requests to inject SQL Query statement
Stealth Commanding	Blocks requests to execute specific commands in the web server through HTTP Request
Suspicious Access	Blocks access which is not fit the standard web browser request
Unicode Directory Traversal	Blocks request of access to directory and files using vulnerabilities related to Unicode manipulation of web server
URI Access Control	Controls requests of access to specific URIs and files
Website Defacement	Detects defacement of websites and recovers the web page.

Appendix D: WAPPLES Product Specifications

Class	Model		Max. Throughput	Network Interface		Memory	Appliance
Value	WAPPLES -50		100 Mbps	2 x 1G Copper port 4 x 1G Copper bypass port		4 GB	
	WAPPLES -100		300 Mbps	2 x 1G Copper port 4 x 1G Copper bypass port	- Optional 4 x 1G Copper bypass port	4 GB	
	WAPPLES -500	U	500 Mbps	2 x 1G Copper port 8 x 1G Copper bypass port		8 GB	
		F	500 Mbps	2 x 1G Copper port 4 x 1G Copper bypass port 2 x 1G Fiber bypass port		8 GB	
Performance	WAPPLES -1200		2 Gbps	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port	- Optional 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port	8 GB	
	WAPPLES -2200		4 Gbps	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port	- Optional 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port	16 GB	
High-End	WAPPLES -5200		10 Gbps	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port	- Optional 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port	24 GB	
	WAPPLES -10000		14 Gbps	2 x 1G Copper port 4 x 1G Copper bypass port or 2 x 1G Copper port 2 x 1G Fiber bypass port or 2 x 1G Copper port 2 x 10G Fiber bypass port	- Optional 4 x 1G Copper bypass port 8 x 1G Copper port 4 x 1G Fiber module port 8 x 1G Fiber module port 2 x 1G Fiber bypass port 2 x 10G Fiber module port 2 x 10G Fiber bypass port	32 GB	

Penta Security Systems Inc.
20th Flr., Hanjin Shipping Bldg., 25-11
Yeoeuido-dong, Yeongdeungpo-gu, Seoul, Korea
Tel. 82-2-780-7728   Fax. 82-2-786-5281

Penta SECURITY
www.pentasecurity.com