Imperva SecureSphere
Web Application Firewall

Alessandro Colombelli
System Engineering
Exclusive-Networks
Next Generation Threats - New Approach

Imperva’s Mission is to Provide a Complete Solution
Web Application Security Use Cases

- **Security and Compliance**
  - Web Application Protection

- **IT Operations**
  - Application Virtual Patching
  - DDoS Protection

- **Line of Business**
  - Site Scraping Prevention
  - Fraud Prevention
  - Legacy Application Security
  - Hosted Application Protection
Web Application Protection Use Case

Anonymous Attack on Customer Site

SecureSphere stopped all phases of attack

PHASE I
Technical Attack

PHASE II
Technical Attack

PHASE III
Business Logic Attack

Recruiting and Recon

APP DDoS Attack

SQL Injection XSS, RT

Scanners such as Nikto

Havij SQL injection tool

LOIC application
The Defenses Required to Protect Web Apps

- Dynamic Profiling
- Attack Signatures
- HTTP Protocol Validation
- Cookie Protection
- IP Reputation
- Anti-Scraping Policies
- Bot Mitigation Policies
- IP Geolocation
- Web Fraud Detection

**Technical Attack Protection**

**Business Logic Attack Protection**

**Fraud Prevention**
Phase I: Attack Signatures Detect Recon and Attacks

The Imperva ADC investigates new threats reported around the world.

SecureSphere appliances updated with latest defenses.

SecureSphere appliances detect scanner agent & attacks.

GET /script>alert('vulnerable')</script> HTTP/1.1
User-Agent: Mozilla/4.75 (Nokia2-1.4) (Evasions:none) (Test:001184)
Connection: Keep-Alive
Host: 11.11.20.131

Signatures detect scanner agent & attacks.
Phase II: SecureSphere Stops SQL Injection, XSS

Advanced analysis drastically reduces false positives and negatives
Phase III: How SecureSphere Stops Application DDoS

- Low-Orbit Ion Cannon (LOIC) DDoS Tool
  - Creates 200 requests per second per browser window

Custom DDoS policy detects excessive requests in a period, malformed URL, unknown HTTP method
In 2011, an enterprise:

- Suffered SQL injection by LulzSec
- Had traditional network security, but NO WAF

Impact:

- 101M records breached
- Fines, lawsuits
- Cost: $200M - $1Billion
IPS & NG Firewall Web Security Features

- Dynamic Profiling
- Attack Signatures
- HTTP Protocol Validation
- Web Fraud Detection
- Correlated Attack Validation
- IP Geolocation
- IP Reputation
- Anti-Scraping Policies
- Bot Mitigation Policies
- Technical Attack Protection
- Business Logic Attack Protection
- Fraud Prevention

- High rate of false positives and negatives because of lack of app awareness
- Easy for hackers to evade via encoding, custom app vulnerabilities
By analyzing traffic, SecureSphere automatically learns...

So it can alert on or block abnormal requests
Dynamic Profiling Over Time

- Cuts deployment time from months to days
- Eliminates ongoing administration burden
  - 5-15 changes per week equals 5-30 man hours of configuration

Understands the application and usage
Adapts to ongoing application changes
How ThreatRadar Reputation Works

1. Collects attack data from WAF community & 3rd party providers

2. Distributes feeds to SecureSphere WAF

3. Blocks malicious sources and emerging threats
Restrict Access By Country

- IP geolocation enables monitoring and blocking by country
  - Can be combined with bot rules for granular control
  - Reduces unwanted traffic to Website
- Geolocation helps with export compliance (EAR, OFAC)
  - Banks may be fined for wire transfers to sanctioned countries
Site Scraping Use Case

Financial company’s challenges:
- Site scrapers copy and republish the stock picks
- Spammers inject ads into forums
- Existing IPS “just created noise”

SecureSphere WAF:
- Blocks scraping and comment spam
- Accurately stops Web attacks
Defenses to Stop Site Scraping

- **Bot mitigation technology** detects scraping bots
- **Anti-scraping policy** detects excessive unique page requests
- **Custom rules** combine multiple defenses
Virtual Patching Use Case

Challenges for payment processor:
- Costly, time-consuming vulnerability fix cycles
- Target of Web attacks

Company scans site with app scanner

Vulnerabilities imported into WAF

SecureSphere:
- Reduces window of exposure, cost of manual app fixes
- Offers visibility for developers
Virtual Patching Through Scanner Integration

- SecureSphere can import scan results and instantly create mitigation policies
- Eliminated payment processors’ emergency fix and test cycles

Scanner finds vulnerabilities

Web applications are protected

SecureSphere imports scan results

© 2013 Imperva, Inc. All rights reserved. Confidential
Quickly & Cost Effectively Secure Applications

- **116 Days**: average time to fix all vulnerabilities\(^1\)

- SecureSphere’s default security policies and virtual patching reduces window from **116 days to 0-5 days**

- SecureSphere can mitigate vulnerabilities not found by scanners

\(^1\) WhiteHat Website Security Statistics Report, Winter 2011
Improve Application Development Processes

Software Development Lifecycle

**DESIGN & CODE**
- Architect and implement code
- Fix errors and vulnerabilities

**TEST**
- Test for vulnerabilities
  - Virtually patch vulnerabilities

**DEPLOY**
- Block attacks
- Monitor and report exploits
- Detect leaks, errors

- Imperva SecureSphere
- Manual processes or third party tools
Fraud Prevention Use Case

A bank needed to:
- Stop Man-in-the-Browser attacks & high risk transactions
- Address FFIEC compliance

SecureSphere Tracks Fraud Details

<table>
<thead>
<tr>
<th>Web Fraud Detection Results: Trusteer Pinpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Malware Details</td>
</tr>
<tr>
<td>Malware Detected</td>
</tr>
</tbody>
</table>

ThreatRadar Fraud Prevention:
- Detected malware and suspicious devices
- Required no changes to apps for initial rollout or policy changes
ThreatRadar Fraud Prevention

SecureSphere integrates with Trusteer, ThreatMetrix, and iovation to detect fraud malware and fraudulent devices

1. User accesses Website
2. SecureSphere redirects browser to ThreatRadar Cloud
3. Browser downloads code, checks device
4. Result sent to WAF
DDoS Protection Use Case

**RV manufacturer:**
- Received DDoS that took down Website for 3 days

**Imperva Incapsula:**
- Stopped SYN Flood in less than 2 hours from phone call
- Stopped follow-on attack

**DDoS attack traffic is blocked**
Imperva Incapsula DDoS Protection

- Stops all DDoS threats
  - Application & network attacks
  - Proprietary technology differentiates humans from bots
    - Analyzes HTTP redirect, cookie, and JavaScript execution capabilities

- Scales beyond your Internet connection limit
  - Stops multi-gigabit DDoS attacks
Hosted Application Protection Use Case

Retailer:
- Had upcoming PCI audit
- Needed to protect Website and meet PCI 6.6
- Hosted apps in the cloud

Imperva Incapsula:
- Helped retailer meet PCI
- Fast, easy deployment

Imperva Incapsula Dashboard

Company’s Website

Legitimate Users

Scrapers

Spammers

Bots

Hackers
Deployment and Management
Inline, Non-inline, and Virtual Options
Broadest Deployment Options in Industry

- **Transparent inline bridge**
  - Supports full enforcement
  - High performance, low latency
  - Fail-open interfaces
- **Transparent and reverse proxy**
  - High performance for content modification
  - URL rewriting, cookie signing, SSL termination
- **Non-inline deployment**
  - Primarily for monitoring, zero network latency
Scalable Centralized Management

- **MX Management Server**
  - Centralized management for Web, database and file products
  - Integrated alerting and reporting

- **Granular role-based access**
  - LDAP, Certificate Auth

- **SecureSphere Operations Manager**
  - Manager of Managers
  - System-wide health monitoring
Real-time Dashboard

The configurable live dashboard shows...

- System utilization
- The latest security alerts
- And system events
Graphical Security Reports

- Pre-defined reports
- Custom reports
- Reports created on demand or emailed daily, weekly, or monthly
- PDF and CSV (Excel) format
- Integration with 3rd party reporting and SIEM tools
Imperva Web Application Security Products

SecureSphere Web Application Firewall
Accurate, automated protection against online threats

Reputation Services
Near real-time user reputation data stops bots and automated attacks

Fraud Prevention
Block Man-in-the-Browser attacks and fraudulent devices

Incapsula
- Simple, affordable cloud-based Web application firewall service
- Ironclad DDoS protection
- Website performance acceleration
Imperva SecureSphere Advantages

**Accuracy**
With multiple layers of defense and correlation

**Application Security Knowledge**
With security research from the Imperva ADC

**Centralized Management**
Unified configuration, monitoring, and reporting

**Transparent Deployment**
Drop-in deployment with bridge, proxy & non-inline

**End-to-End Protection**
For Web applications, databases and files
Complete Protection Against Web Threats

SecureSphere

- Bots
- Web Attacks
- Known Attackers
- Undesirable Countries
- Vulnerabilities
- Web Fraud
- Web Apps
- Business Logic Attack Protection
- Fraud Prevention
- Virtual Patching
- Technical Attack Protection

Scrapers
DDoS
App DDoS
Phishing Sites
Comment Spammers
Spammers
Q & A
Thank You