Securing your Applications & Data
With
Web Application Firewalls

Dennis K. Usle
Sr. Security Architect, Radware
July 2013
Cyberwar: The Web App Aspect
Web Application Security Challenge
Countermeasure: WAF
Selection Considerations
Cyber War: The Web Application Aspect
Cyberwar Toolbox

- Gathering & Manipulating Data
- Web Vandalism
- Cyber Espionage
- Disruption of Service
- Attack Critical Infrastructure
- Trojan, Viruses & Worms
Targeting Different Layers

- Large volume network flood attacks
- Network scan
- Intrusion
- Port scan, SYN flood attack
- OS Commanding
- “Low & Slow” DoS attacks (e.g. Sockstress)
- Application vulnerability, malware
- High and slow Application DoS attacks
- XSS, Brute force
- SQL Injection, LDAP Injections
- XML manipulations, Web Services Abuse
- Leakage of Sensitive Data
Approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

McAfee, 2007,
The Internet security report
The ongoing cyberwar between India and Bangladesh has escalated with Teamgreyhat, in support of “our Indian brothers”, moving from commercial to economic targets.

Taiwan plans to beef up its cyberwar capabilities to counter a perceived threat from Chinese hackers targeting government and security websites.

The Pentagon is digging in on the cyberwar front, with an elite school run by the Air Force training officers to hunt down hackers and launch electronic attacks.
Cyberwar – The Web App Aspect
Web Applications Security Challenge
Web Apps are Easy to Exploit

- Whole system open to attack
- Can target different layers
- Thousands of Web security vulnerabilities
- Minimal attention to security during development
- Traditional defences inadequate

All they need is a browser
Thousands of Vulnerabilities Every Year

# of Vulnerabilities

- Source: National Vulnerabilities Database
Minutes to Compromise, Months to Discover

- Initial Attack to Initial Compromise: 
  - Seconds: 10% (0%), Minutes: 75% (38%), Hours: 12%, Days: 2%, Weeks: 0%, Months: 1%
- Initial Compromise to Data Exfiltration: 
  - Seconds: 8%, Minutes: 38%, Hours: 14%, Days: 25%, Weeks: 8%, Months: 8%
- Initial Compromise to Discovery: 
  - Seconds: 0%, Minutes: 0%, Hours: 2%, Days: 13%, Weeks: 29%, Months: 54%
SQL Injections are Dominant
Trends for Web App Vulnerability Types

![Bar chart showing trends for web app vulnerability types.]

- Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery

Categories shown:
- Financials
- Government
- Industrial
- Info. Tech
- Logistics

% Finding Likely to Occur in Test
Top Attack Methods

Source: webappsec.org
Web Site Defacements (before)

The City of Detroit's website before any defacement event. The image shows the website's front page, which includes a banner with a message about Angel's Night efforts, a section for City Services, and various news and projects related to the city.
Sep 9, 2012

Dominos Pizza (India)

37,187 names, phone numbers, email addresses, passwords and addresses
Jan 31, 2011: “Online dating Web site PlentyOfFish.com has been hacked, exposing the personal information and passwords associated with almost 30 million accounts.”
Top Web Attack Impacts

- Source: webappsec.org
The average total cost of a data breach rose to $6.75 million in 2009.
Records of sensitive information (CCN, SSN, etc.) were breached by hacking attempts only in the United States.

The population of the United States, projected to Sep 2012 is 314,324,529

315,112,297 Records in our database from 718 Breaches made public fitting this criteria
Source of Breach

- 80% External
- 18% Partner
- 2% Internal

Source: 7safe.com
Countermeasures:
Web Application Firewall
DoS Protection

Behavioral Analysis

IPS

IP Rep.

WAF

Mapping Security Protection Tools

Large volume network flood attacks

Network scan

Intrusion

Port scan, SYN flood attack

OS Commanding

“Low & Slow” DoS attacks (e.g. Sockstress)

Application vulnerability, malware

High and slow Application DoS attacks

XSS, Brute force

SQL Injection, LDAP Injections

XML manipulations, Web Services Abuse

Leakage of Sensitive Data

SHUT DOWN
Cost Effective, Time to Security

Time to Fix (Days)

- SQL Injection: 138 days
- Insufficient Authorization: 59 days
- HTTP Response Splitting: 104 days
- Directory Traversal: 105 days
- Insufficient Authentication: 160 days
- Insufficient Authentication: 88 days
- Cross Site Scripting: 92 days
- Abuse of Functionality: 123 days
- Session Fixation: 23 days
- Cross Site Request Forgery: 17 days
- HTTP Response Splitting: 36 days
- Information Leakage: 114 days
- Content Spoofing: 85 days
- Predictable Resource Location: 128 days
- Directory Indexing: 87 days

Source: WhiteHat Security
Security Intelligence Timeline

Vulnerability → Exploit

What are the internal/external threats?

Can we protect against there threats?
Why WAF

- Time to Security
- Centralized Security
- Protect 3rd Party Modules
- No App Modification
- Security While App Changes
- Application Visibility

Cost Effective
WAF Selection Considerations
Zero Day vs. Know attacks

False Negative vs. False Positive

Time to Security

Auto Policy Generation

Performance / Scalability
Mapping Your Requirements - Advanced

- Cost of Ownership
- Changes to Existing Environment
- Inline vs. out-of-path
- Reverse Proxy vs. Bridge
- Level of Protection
Data Leak Prevention
- Credit card number (CCN) / Social Security (SSN)
- Regular Expression

Terminate TCP, Normalize, HTTP RFC
- Evasions
- HTTP response splitting (HRS)

Signature & Rule Protection
- Cross site scripting (XSS)
- SQL injection, LDAP injection, OS commanding
Advanced Web Application Protection

- **Parameters Inspection**
  - Buffer overflow (BO)
  - Zero-day attacks

- **User Behavior**
  - Cross site request forgery
  - Cookie poisoning, session hijacking

- **Layer 7 ACL**
  - Folder / file level access control
  - White listing or black listing

- **XML & Web Services**
  - XML Validity and schema enforcement

- **Role Based Policy**
  - Authentication
  - User Tracking
Priorities make things happen.
Summary

Smart Network. Smart Business.
Cyberwar: The Web App Aspect
Web Application Security Challenge
Countermeasure: WAF
Selection Considerations
NBA
- Prevent application resource misuse
- Prevent zero-minute malware

DoS Protection
- Prevent all type of network DDoS attacks

Reputation Engine
- Financial fraud protection
- Anti Trojan & Phishing

IPS
- Prevent application vulnerability exploits

WAF
- Mitigating Web application threats and zero-day attacks
Thank You