Keeping the Bad Guys Out—Safeguarding Applications and Data

Susann Ulrich – North America Security Practice Leader, Rational Software
sulrich@us.ibm.com
Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information
Smarter planet opportunities driven by Web-enabled applications

The Opportunity – smarter planet

Globalization and Globally Available Resources

Access to streams of information in the Realtime

Billions of mobile devices accessing the Web

New Forms of Collaboration
The Costs from Security Breaches are Staggering

143 MILLION RECORDS COMPROMISED IN 2009

$214 COST PER COMPROMISED RECORD

AVG COST TO ORGANIZATION FOR A BREACH $7.2 MILLION

Verizon 2010 Data Breach Investigations Report

2010 Annual Study: U.S. Cost of a Data Breach – Ponemon Institute LLC

2010 Annual Study: U.S. Cost of a Data Breach – Ponemon Institute LLC
Sources of Security Breach Costs

Unbudgeted Costs:
- Customer notification / care
- Government fines
- Litigation
- Reputational damage
- Brand erosion
- Cost to repair
The Evolution of the Security Landscape

Early 90s

- Fun & personal glory
- Light website
- Network level vulnerabilities
  - Organizations got better at firewalls, using switch technology and encryption

Now

- Critical data & business
- $$$
- Application level vulnerabilities
- Critical data & business
- Application level vulnerabilities
- System level vulnerabilities
  - OS vendors such as Microsoft and Linux have scrubbed out most of the defects in the OS code
- System code level vulnerabilities
  - It's the thousands of applications, produced by thousands of software makers, that make up this huge 4th wave.
  - OS vendors started locking down their systems out of the box and users started to get better at managing security configurations
Hackers Continue to Focus on Web Applications

… because they are easy points of entry and there is valuable data exchanged in the business processes run by the applications

Web Application Vulnerabilities on the Rise

Source: 2010 IBM ISS X-Force Mid Year Report
Hackers Continue to Focus on Web Applications

Web Application Vulnerabilities on the Rise

- Unfortunately, it appears that the volume of SQL injection disclosure is back up during the first half of 2010.
- Over half (55 percent) of all vulnerabilities disclosed in the first half of 2010 have no vendor-supplied patch at the end of the period.

Source: 2010 IBM ISS X-Force Mid Year Report
2010 Breach Trends

WHO IS BEHIND DATA BREACHES?

- 70% resulted from external agents (-9%)
- 48% were caused by insiders (+26%)
- 11% implicated business partners (-23%)
- 27% involved multiple parties (-12%)

HOW DO BREACHES OCCUR?

- 48% involved privilege misuse (+26%)
- 40% resulted from hacking (-24%)
- 38% utilized malware (<>)
- 28% employed social tactics (+16%)
- 15% comprised physical attacks (+6%)

WHAT COMMONALITIES EXIST?

- 98% of all data breached came from servers (-1%)
- 85% of attacks were not considered highly difficult (+2%)
- 61% were discovered by a third party (-8%)
- 86% of victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls (+9%)
- 79% of victims subject to PCI DSS had not achieved compliance

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT
2010 Breach Trends

Figure 14. Threat action categories by percent of breaches and records

- Malware: 38% / 94%
- Hacking: 40% / 96%
- Social: 28% / 3%
- Misuse: 48% / 3%
- Physical: 15% / 1%
- Error: 2% / 0%
- Environmental: 0% / 0%

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT
2010 Breach Trends

Hacking (40% of breaches, 94% of records)

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT
2010 Breach Trends

![Graph showing types of hacking by percent of breaches within hacking and percent of records.]

- Use of stolen login credentials: 38% / 86%
- Exploitation of backdoor or command/control channel: 29% / 5%
- SQL Injection: 25% / 89%
- Brute force and dictionary attacks: 14% / <1%
- OS Commanding: 14% / 5%
- Exploitation of default or guessable credentials: 11% / <1%
- Footprinting and Fingerprinting: 11% / <1%
- Cross-site Scripting: 9% / 2%
- Exploitation of insufficient authentication (i.e., no login required): 7% / 2%
- Exploitation of insufficient authorization (weak or misconfigured access control): 7% / <1%
- Remote File Inclusion: 2% / <1%
- DoS at the application layer (consumes system resources): 2% / <1%
- Man-in-the-Middle Attack: 2% / <1%
- Encryption Brute Forcing: 2% / <1%
- Unknown: 5% / <1%

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT
2010 Breach Trends

Figure 22. Attack pathways by percent of breaches within Hacking and percent of records

- Web application: 54% / 92%
- Remote access and control services/software: 34% / 2%
- Backdoor or control channel: 23% / 5%
- Network file/resource sharing services: 4% / 1%
- Physical access or connection: 2% / <1%
- Wireless network: 2% / <1%
- Unknown: 7% / <1%

Source: VERIZON 2010 DATA BREACH INVESTIGATIONS REPORT
Understanding the Web Application

**Organization**

- **Application Development**
  - Requirements
  - Secure Design
  - Dynamic Analysis
  - Static Analysis

- **Secure Hosting Environment**
  - Backend Server
  - Database
  - Application Server
  - Web Server
  - Vulnerability management
    - Network
    - Host
    - Application
  - Incident & event management
  - Identity & access management
  - Malware detection

- **Defend Network**
  - Firewall
  - IDS / IPS
  - Web App Firewall
  - Anti-virus

- **Protect Data across Internet**
  - SSL Encryption

**Client**

- **Desktop**
  - Anti-virus
  - Anti-malware
  - Personal firewall

- **Client**
  - Anti-virus
  - Anti-malware
  - Personal firewall
Attack Vectors

- Attacks against the Browser
- Attacks against the Application
- Attacks against the Database
- Eavesdropping on the Network
- Attacks against the Server
Why are Web Applications so Vulnerable?

- Developers are mandated to deliver functionality on-time and on-budget - but not to develop secure applications
- Developers are not generally educated in secure code practices
- Product innovation is driving development of increasingly complicated software for a Smarter Planet
- Network scanners won’t find application vulnerabilities and firewalls/IPS don’t block application attacks

Volumes of applications continue to be deployed that are riddled with security flaws…

...and are non compliant with industry regulations
Perimeter defenses no longer sufficient

“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”

-- William J. Lynn III, U.S. Deputy Defense Secretary
Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information
<table>
<thead>
<tr>
<th>OWASP Top 10 Threat</th>
<th>Negative Impact</th>
<th>Example Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross Site Scripting</td>
<td>Identity Theft, Sensitive Information Leakage, Browser control</td>
<td>Hackers can impersonate legitimate users, and control their accounts.</td>
</tr>
<tr>
<td>Injection Flaws</td>
<td>Attacker can manipulate queries to the DB / LDAP / Other system</td>
<td>Hackers can access backend database information, alter it or steal it.</td>
</tr>
<tr>
<td>Malicious File Execution</td>
<td>Execute shell commands on server, up to full control</td>
<td>Site modified to transfer all interactions to the hacker.</td>
</tr>
<tr>
<td>Insecure Direct Object</td>
<td>Attacker can access sensitive files and resources</td>
<td>Web application returns contents of sensitive file (instead of harmless one).</td>
</tr>
<tr>
<td>Reference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross-Site Request Forgery</td>
<td>Attacker can invoke “blind” actions on web applications, impersonating as a trusted user</td>
<td>Blind requests to bank account transfer money to hacker.</td>
</tr>
<tr>
<td>Information Leakage and</td>
<td>Attackers can gain detailed system information</td>
<td>Malicious system reconnaissance may assist in developing further attacks.</td>
</tr>
<tr>
<td>Improper Error Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broken Authentication &amp;</td>
<td>Session tokens not guarded or invalidated properly</td>
<td>Hacker can “force” session token on victim; session tokens can be stolen after logout</td>
</tr>
<tr>
<td>Session Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insecure Cryptographic</td>
<td>Weak encryption techniques may lead to broken encryption</td>
<td>Confidential information (SSN, Credit Cards) can be decrypted by malicious users</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insecure Communications</td>
<td>Sensitive info sent unencrypted over insecure channel</td>
<td>Unencrypted credentials “sniffed” and used by hacker to impersonate user.</td>
</tr>
<tr>
<td>Failure to Restrict URL Access</td>
<td>Hacker can access unauthorized resources</td>
<td>Hacker can forcefully browse and access a page past the login page.</td>
</tr>
</tbody>
</table>
Cross-Site Scripting (XSS)

- **What is it?**
  - Malicious script echoed back into HTML returned from a trusted site, and runs under trusted context

- **What are the implications?**
  - Session Tokens stolen (browser security circumvented)
  - Complete page content compromised
  - Future pages in browser compromised
XSS Demonstration

Search Results

No results were found for the query:

<asp:literal id="Literal8"><% Response.Write(Request.Form["txtSearch"]%></asp:literal>

HTML code:

<p>No results were found for the query:<br />
<asp:literal id="Literal8">asdf</asp:literal></p>
XSS Demonstration

HTML code:

```html
<p>No results were found for the query:<br />
<span id="ctl00_ctl10_Content_Main_lblSearch"><script>alert(document.cookie)</script></span></p>
```
Cross Site Scripting – The Exploit Process

1) Link to bank.com sent to user via E-mail or HTTP

2) User sends script embedded as data

3) Script/data returned, executed by browser

4) Script sends user’s cookie and session information without the user’s consent or knowledge

5) Evil.org uses stolen session information to impersonate user
Injection Flaws

- What is it?
  - User-supplied data is sent to an interpreter as part of a command, query or data.

- What are the implications?
  - SQL Injection – Access/modify data in DB
  - XPath Injection – Access/modify data in XML format
  - SSI Injection – Execute commands on server and access sensitive data
  - LDAP Injection – Bypass authentication
  - MX Injection – Use mail server as a spam machine
  - HTTP Injection – Modify or poison web caches
  - Etc.
SQL Injection Illustrated

Account: 876398' or '1'='1
All records are returned

HTTP Request

Intrusion detection, firewalls, and hardened OS's won't detect or prevent most application attacks

© 2010 IBM Corporation
Night Dragon

- Successful attacks on 5+ global oil & gas co’s
- Attacks began with SQL-injection, which compromised external web servers
  - Common hacking tools were then used to access intranets, giving attackers access to internal servers and desktops
  - Usernames and passwords were then harvested and after disabling Internet Explorer proxy settings
  - Hackers were able to establish direct communication from infected machines to the Internet.
Agenda

- Current Trends in Application Security
- Understanding Attacks
- Protecting Data and Information
The Framework identifies five security focus areas as starting points:

- **PEOPLE AND IDENTITY**: Mitigate the risks associated with user access to corporate resources.
- **DATA AND INFORMATION**: Understand, deploy, and properly test controls for access to and usage of sensitive data.
- **APPLICATION AND PROCESS**: Keep applications secure, protected from malicious or fraudulent use, and hardened against failure.
- **NETWORK, SERVER AND END POINT**: Optimize service availability by mitigating risks to network components.
- **PHYSICAL INFRASTRUCTURE**: Provide actionable intelligence on the desired state of physical infrastructure security and make improvements.
IBM Security portfolio can help you meet challenges in each security focus area

<table>
<thead>
<tr>
<th>Framework</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEOPLE AND IDENTITY</td>
<td>Manage identities, Control access to applications, Audit, report and manage access to resources</td>
</tr>
<tr>
<td>DATA AND INFORMATION</td>
<td>Protect Critical Databases, Messaging Security and Content Filtering, Monitor &amp; manage data access, Prevent Data Loss, Encryption</td>
</tr>
<tr>
<td>NETWORK, SERVERS &amp; ENDPOINTS</td>
<td>Protect Servers, Endpoints, Networks, Mainframes</td>
</tr>
<tr>
<td>PHYSICAL INFRASTRUCTURE</td>
<td>Video Surveillance, Command and Control, Video Analytics</td>
</tr>
</tbody>
</table>
Protect your most valuable information

Continuously monitor access to high-value databases to:

1. **Prevent data breaches**
   Mitigate external and internal threats

2. **Ensure the integrity of sensitive data**
   Prevent unauthorized changes to sensitive data or structures

3. **Reduce cost of compliance**
   Automate and centralize controls
   1. Across PCI DSS, data privacy regulations, HIPAA/HITECH, ...
   2. Across databases and applications
   Simplify processes

92% of all breached records originate in database servers *(2010 Data Breach Report)*
Addressing the full database security lifecycle

- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

- Automated & centralized controls
  - Cross-DBMS audit repository
  - Preconfigured policies/reports
  - No database changes
  - Minimal performance impact
  - Sign-off management
  - Entitlement reporting

- Assess static and behavioral database vulnerabilities
  - Configuration auditing
  - Preconfigured tests based on best practices standards (STIG, CIS, CVE)
Thank You
IBM Corporation 2010

- IBM, the IBM logo, ibm.com, AppScan, DataPower, Rational, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), these symbols indicate US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

- Other company, product and service names may be trademarks or service marks of others.

- References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.