

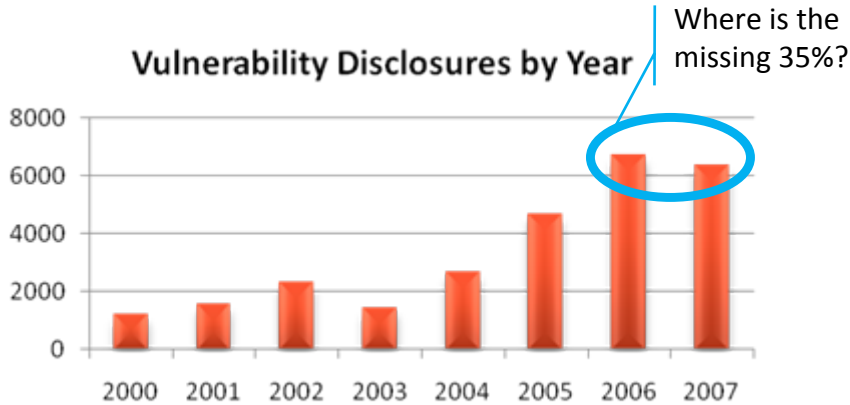
THE BUSINESS OF CYBER VULNERABILITIES

Aaron Turner – CISSP, CISM

Idaho National Laboratory & I³ Partners

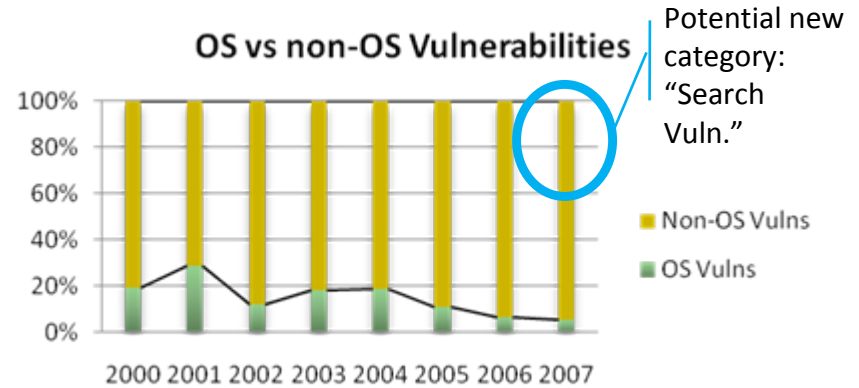
Vulnerability Growth: 2000-2007

A historical view of the volume of security problems that have impacted computing systems in the last 7 years.



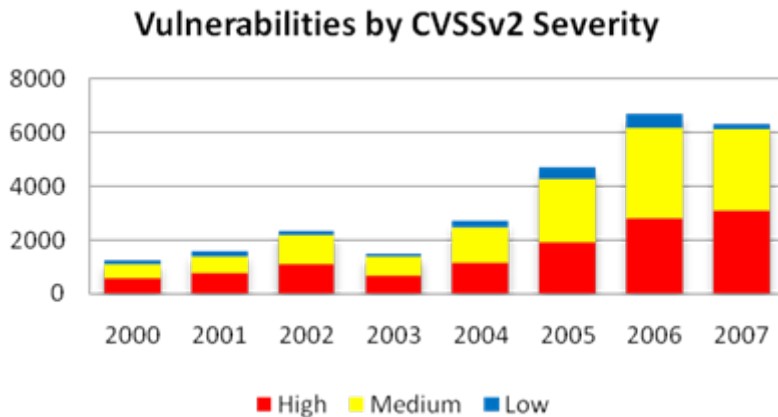
Vulnerability Trends

'Ubiquitous Applications' like Acrobat and Flash are providing new exploitation opportunities.



Severity Increasing

Increasing attacker efficiency is shown in the number and percentage of high-severity vulnerabilities that can be used for targeted attacks.



Industry-wide Problem

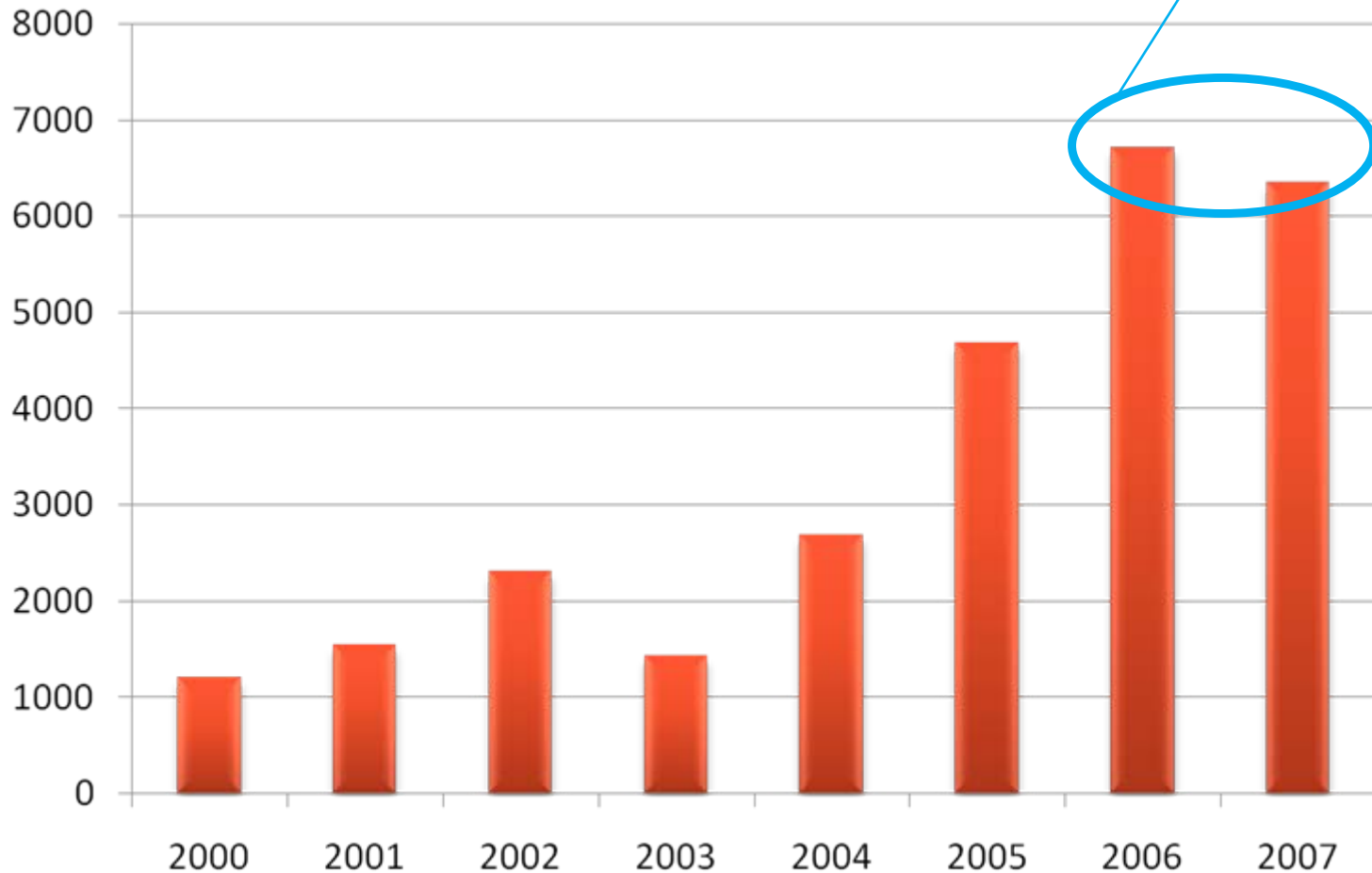
Skilled attackers are equal-opportunity exploiters. A listing of high-severity vulnerabilities from 2007 shows just how pervasive the problem is.

Vendor	Vulnerabilities	Percentage
Microsoft	148	4.3%
Novell	132	3.8%
Red Hat	127	3.7%
Ubuntu	115	3.3%
Apple	110	3.2%
Sun	85	2.5%
PHP	72	2.1%
Oracle	68	2.0%
Cisco	62	1.8%
Mozilla	48	1.4%

Full Point Increase vs '06

Vulnerability Growth 2000 - 2007

A historical view of the volume of security problems that have impacted computing systems in the last 7 years.



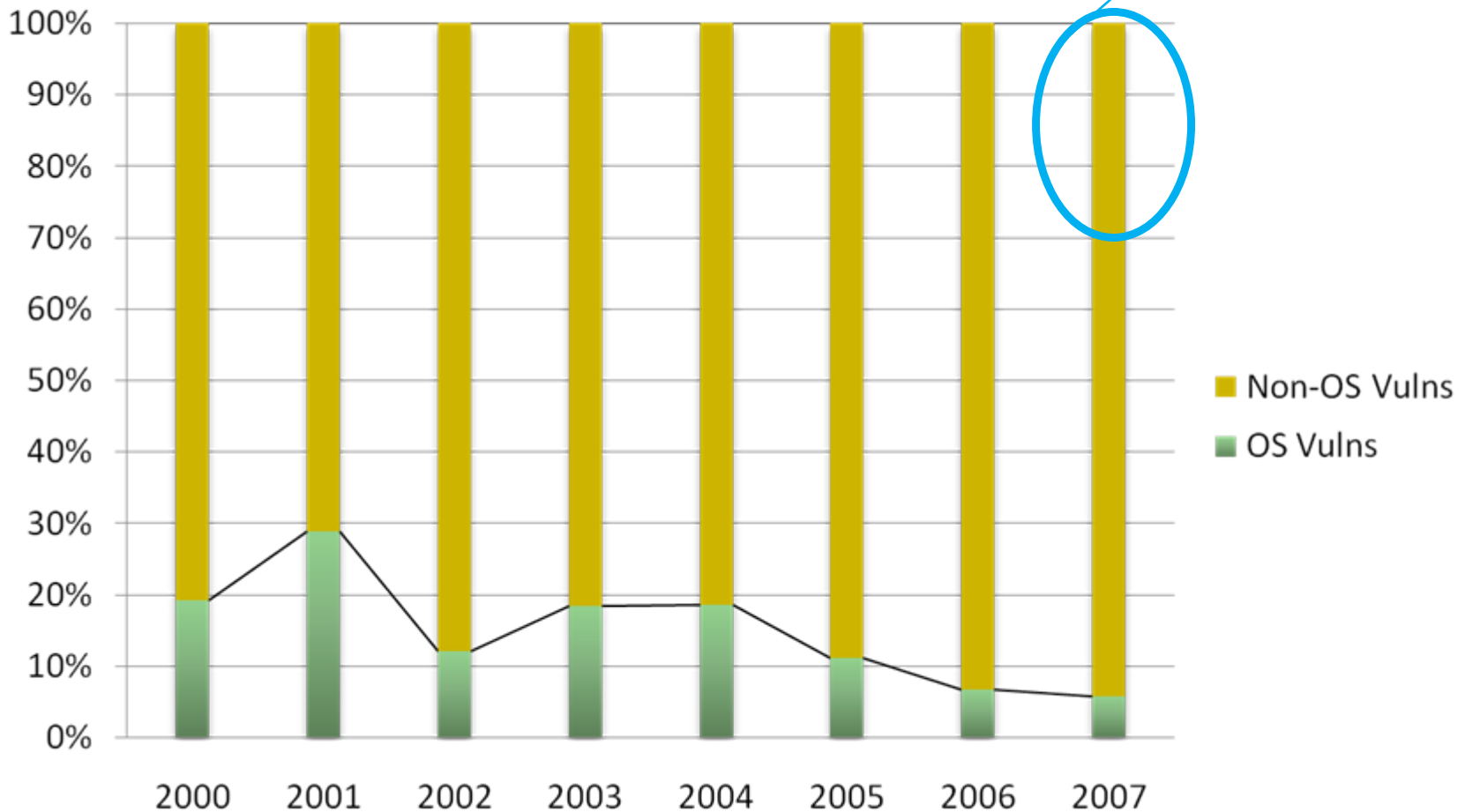
Where is the missing 35%?

Vulnerability Trends

‘Ubiquitous Applications’ like Acrobat and Flash are providing new exploitation opportunities.

Potential new “Search” class of vuln.

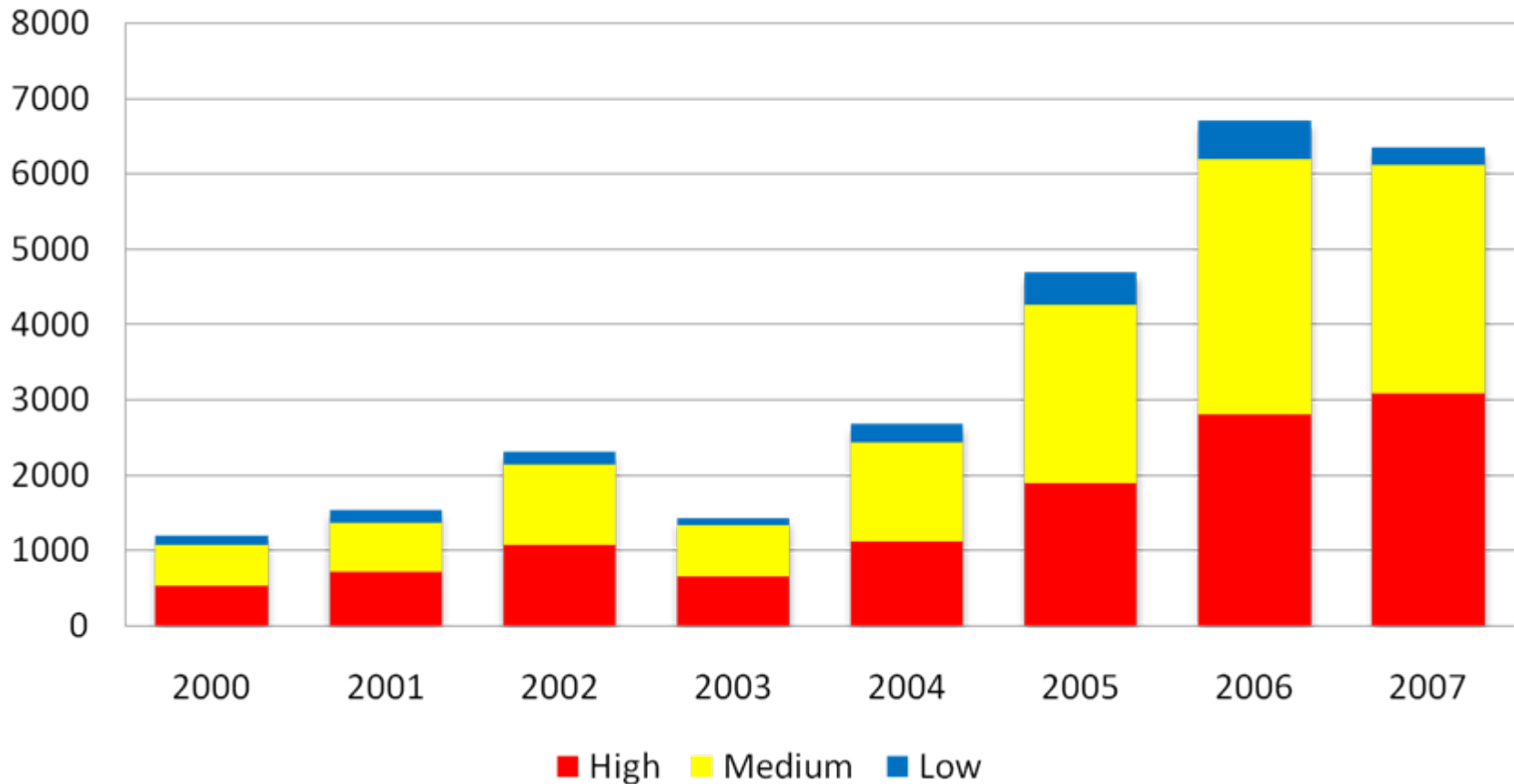
OS vs non-OS Vulnerabilities



Severity Increasing

Increasing attacker efficiency is shown in the number and percentage of high-severity vulnerabilities that can be used for targeted attacks.

Vulnerabilities by CVSSv2 Severity



Equal Opportunity

Skilled attackers are equal-opportunity exploiters. A listing of high-severity vulnerabilities from 2007 shows just how pervasive the problem is.

Vendor	Critical Vuln's	%
Microsoft	148	4.3%
Novell	132	3.8%
Red Hat	127	3.7%
Ubuntu	115	3.3%
Apple	110	3.2%
Sun	85	2.5%
PHP	72	2.1%
Oracle	68	2.0%
Cisco	62	1.8%
Mozilla	48	1.4%

Full percentage point increase since '06

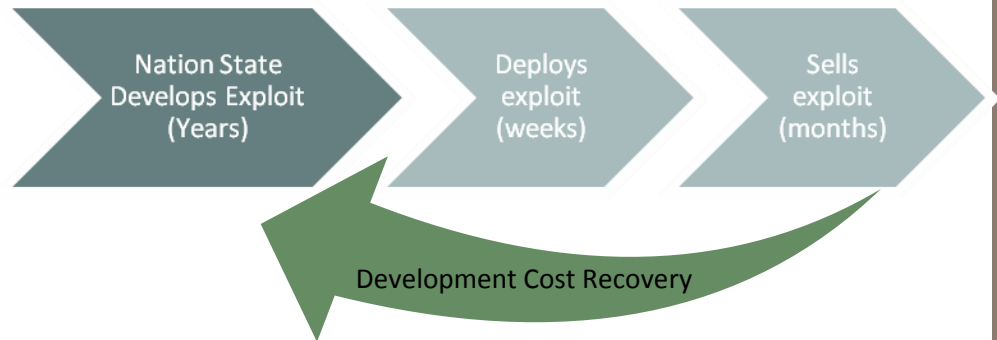
The Economics of Vulnerabilities

- An underground economy has been established for the production, distribution, exchange and purchase of vulnerabilities
- As with any economic system, the attacker community has succeeded in discovering efficiencies through specialization of labor
 - Vulnerability Factories
 - Vulnerability Wholesalers
 - Vulnerability Transporters
 - Vulnerability Consumers
- Examples:
 - 76service.com
 - Executive Phishing Services

The Vulnerability Market

In 2006, a complex vulnerability was discovered through telemetry from Microsoft's sensor networks.

Through further investigation, it was determined that the level of effort required to research the vulnerability and develop the exploit would have required significant effort and manpower. Within weeks of the targeted attack, the exploit was seen for sale within underground economy channels.



Leading Vulnerability Economies: % of Vulnerabilities to # of Total Estimated Computer Users by Country

Asia-Pacific	
Mongolia	25.0%
Thailand	8.2%
Macau SAR	8.1%
Vietnam	7.5%
Indonesia	6.8%

Middle East - Africa	
Bahrain	8.7%
Egypt	7.0%
Iraq	6.9%
Moroco	6.7%
Saudi Arabia	6.7%

Europe	
Albania	8.7%
Turkey	7.1%
Romania	4.6%
Portugal	4.4%
Russia	4.4%

The Americas	
Dom. Republic	9.4%
Brazil	7.4%
Honduras	6.9%
Jamaica	6.2%
Chile	6.1%

Special Thanks to:

Jeff R. Jones, Senior Security Strategist, Microsoft Corporation

All Vulnerability Data Referenced from:

Microsoft Security Intelligence Report

<http://www.microsoft.com/sir>

Additional Resources

Search Vulnerability:

- http://www.usatoday.com/money/industries/technology/2008-03-31-javascript-hackers_N.htm

76service.com

- <http://www.cio.com/article/135500/2>

Executive Phishing Services

- <http://www.informationweek.com/news/showArticle.jhtml?articleID=206103681>

Contact Information

aaron@i3partners.org