

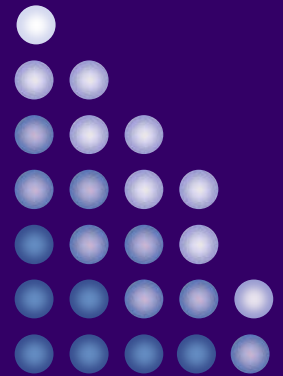
Current Issues: Information Security

Keith A. Watson, CISSP

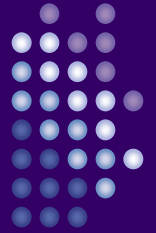
Research Engineer

Center for Education and Research in
Information Assurance and Security

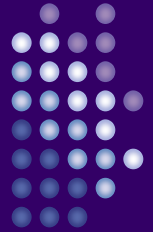
Purdue University



Overview



- CERIAS
- A Brief Intro to Information Security
- Scary Statistics
- New Trends
- Security Challenges

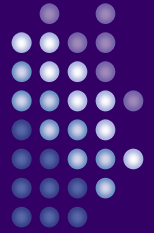


Center for Education and Research in Information Assurance and Security

- Cross-disciplinary
 - 80 faculty / 8 colleges / 20 departments
- 100 Ph.D. and M.S. students
 - Graduates 20% of US annual INFOSEC Ph.D.s
- Eight diverse areas of research
- Supported through corporate and government sponsorships (Cisco, Sun, HP, Microsoft, NRO)
- Serves as an unbiased resource to the world-wide community

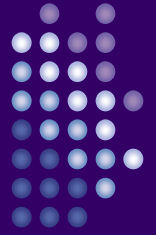
A Brief Intro to Information Security

PURDUE
UNIVERSITY



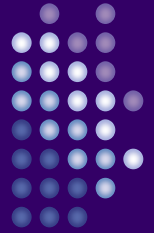
Information Security
is the Process of Protecting
Information and Information
Resources

Risk Management Process



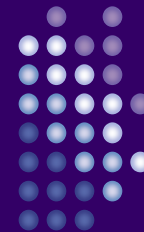
1. Identify Assets
2. Determine Risk
3. Evaluate Current Controls
4. Implement New Controls/Adjust Existing
5. Repeat

Thinking about Information Security



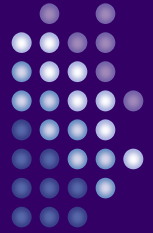
- *Confidentiality*
 - What would happen if sample information were accidentally published to a public web site?
- *Integrity*
 - How reliable would sample information be if it could be modified by anyone on the internet?
- *Availability*
 - How would you get any work done if all the mice disappeared?

2006 Statistics



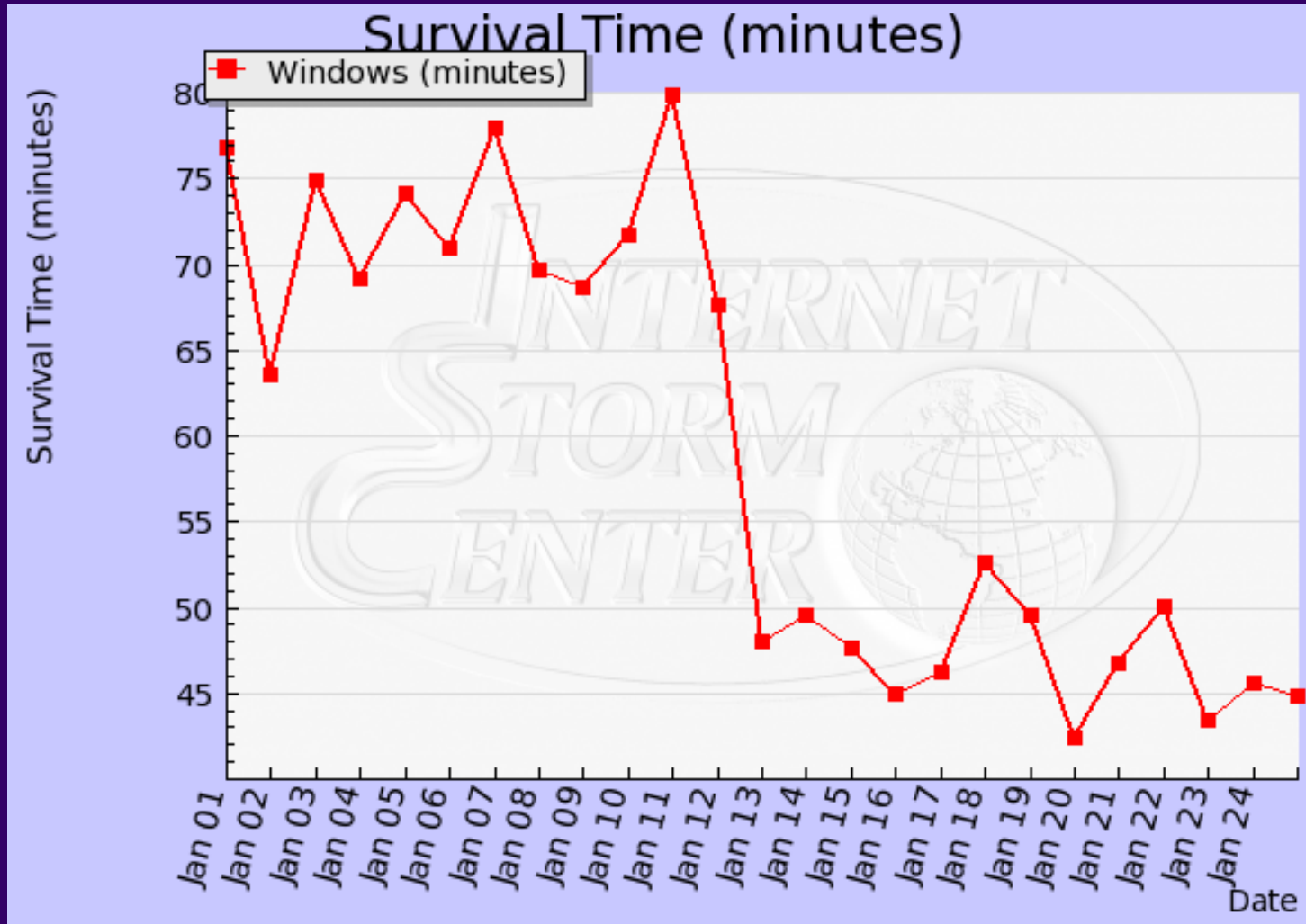
- CERT/CC
 - Vulnerabilities Reported: **8064** (up 35%)
 - Vulnerability Notes: **422** (up 48%)
- National Cyber Alert System
 - Alerts, Tips, Bulletins: **136** (up 31%)
- National Vulnerability Database
 - Vulnerabilities Reported: **6604** (up 35%)
- Symantec Vulnerability Database
 - Vulnerabilities Reported: **4883** (up 30%)

Some Specific Stats

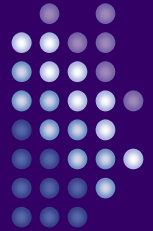


- Microsoft (2006)
 - IE Vulnerable for 284 days
 - Office had 41 critical vulnerabilities
 - MS products had 104 critical vulnerabilities
- Mozilla (2006)
 - Firefox vulnerable for 9 days
- Apple (2007)
 - Mac Quicktime vulnerable for 23 days
 - Windows Quicktime fix still unavailable/inaccessible
- Cisco (2007)
 - Released 8 Security Bulletins in January

Unpatched Windows Survival Time

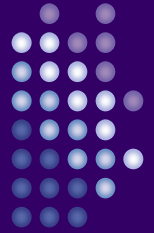


New Trends



- Month of Bugs from the Metasploit Project
 - Month of Browser Bugs (July '06)
 - Month of Kernel Bugs (Nov '06)
 - Month of Apple Bugs (Jan '07)
- Bug Brokers offering Bounties for Bugs
 - Corporate Programs offer \$5k-\$10k
 - Private Buyers offer \$60k-\$120k
- Search Engines for Source Code
 - Krugle.com, Koders.com, Google Code Search
 - Anyone can look for vulnerabilities in hundreds of millions of lines of code (500M LoC in Koders index)

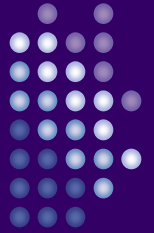
The NPDN Security Challenges



- Threats and Threat-Sources are Evolving
 - Vulnerabilities have value for evil-doers
- Systems are always Vulnerable
 - A system secure today will not be secure tomorrow
- The NPDN is Distributed and Federated
 - Rolling out a top-down security management program is not simple
- People need Security Awareness
 - They are the first line of defense

Q&A

PURDUE
UNIVERSITY



Questions?

kaw@purdue.edu