Carnegie Mellon
Software Engineering Institute

CERT
Coordination
Center

Public Monitoring: *Scouring the Net*

Damon Morda

June 16, 2004

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

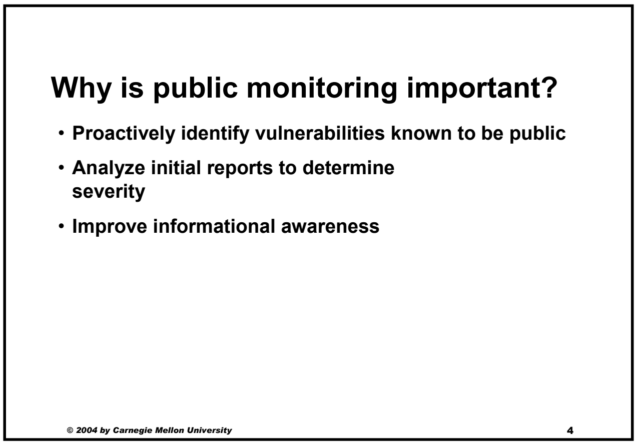
The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.

Agenda

- Public monitoring overview
- Three step process
- Information sources
- Monitoring tools
- Challenges and future improvements

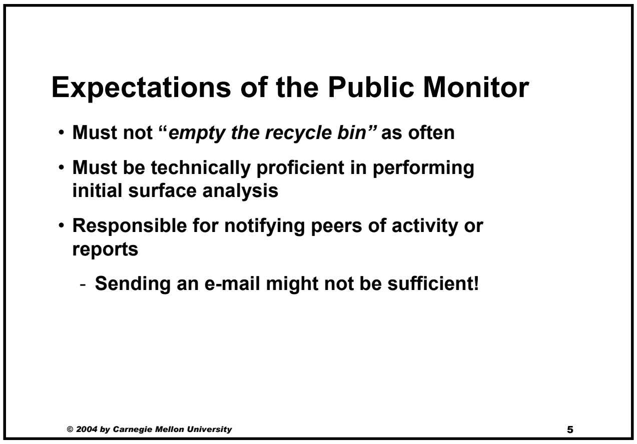
What is public monitoring?

The role of the public monitor is to actively gather vulnerability, incident, and artifact related information from publicly available sources.



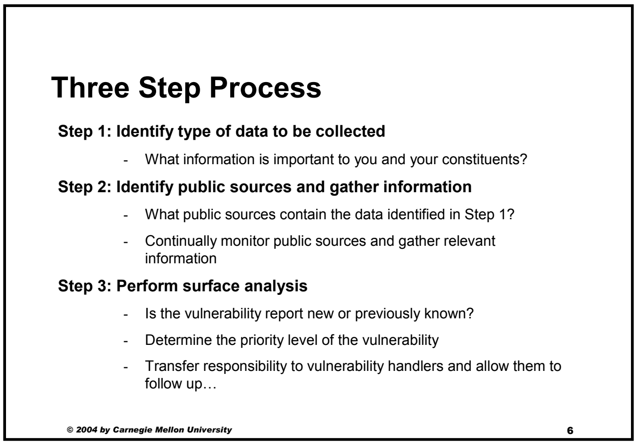
Why is public monitoring important?

- Proactively identify vulnerabilities known to be public
- Analyze initial reports to determine severity
- Improve informational awareness



Expectations of the Public Monitor

- Must not “*empty the recycle bin”* as often
- Must be technically proficient in performing initial surface analysis
- Responsible for notifying peers of activity or reports
  - Sending an e-mail might not be sufficient!



Three Step Process

Step 1: Identify type of data to be collected

- What information is important to you and your constituents?

Step 2: Identify public sources and gather information

- What public sources contain the data identified in Step 1?
- Continually monitor public sources and gather relevant information

Step 3: Perform surface analysis

- Is the vulnerability report new or previously known?
- Determine the priority level of the vulnerability
- Transfer responsibility to vulnerability handlers and allow them to follow up…

Step 1: Identify Data to be Collected

- **What type of information are you and your constituents interested in?**
  - I want everything and anything
    - Vulnerabilities, incidents, and artifacts
  - I want information on technologies used by our constituents
  - I want specific information on vulnerabilities
    - All vulnerability reports or only ones that affect you and your constituents?

Step 2: Gathering Information

- **The Internet and its resources are vast, we better narrow it down a bit…**
  - Mailing lists
  - Newsgroups
  - Vulnerability related web sites
  - Web sites containing security news
- **Narrow the focus to a selected number of reliable sources providing relevant information**

Monitoring Web Sites

- **Security advisory web sites**
  - US-CERT, SecurityFocus, SecuriTeam, Security Tracker, Secunia, OSVDB, vendor web sites
- **Security related news web sites**
  - Slashdot
  - The Register
  - INFOSYSSEC portal (links galore)
- **Mailing list archives**
  - Neohapsis and MARC

Note: Web site links will be provided at the end of the presentation.

Monitoring Mailing Lists

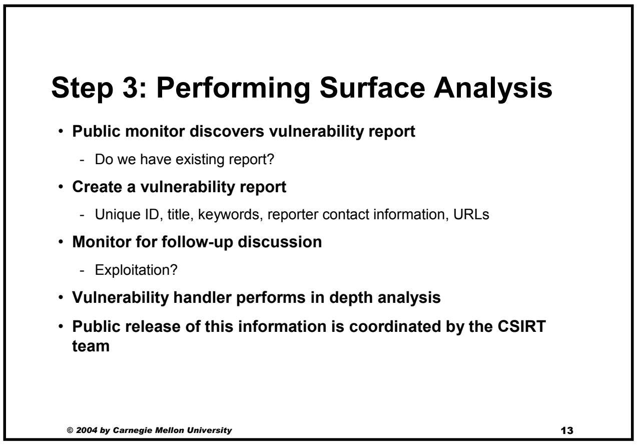
- **Bugtraq, Full-Disclosure, NTBugtraq, Vuln-Dev, vendor announcements**
- **CERT/CC monitors over 80 mailing lists**
- **Some lists have high signal/noise ratio**
- **Mailing list archives (Neohapsis and MARC)**
  - All you need is a web browser

Monitoring 80+ Mailing Lists

- **Subscribe email address to mailing lists**
- **Sort incoming messages based on origin**
- **CERT/CC uses IMAP folders and the Mulberry mail client**
  - Cabinets
  - New Messages
  - Organized information

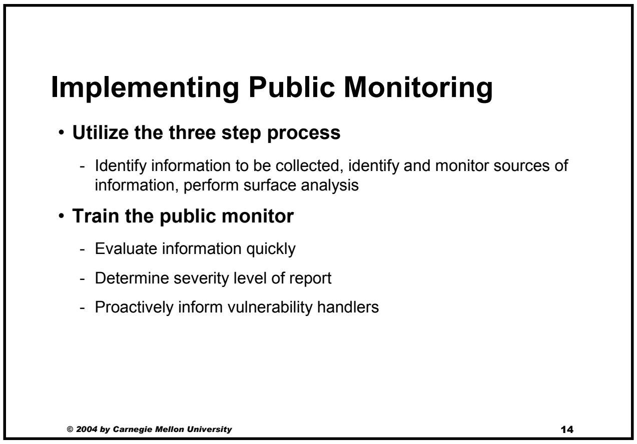
Gathering Vulnerability Reports

- **A vulnerability report is a report of a bug, flaw, or defect in a software or hardware product that may impact the security of that product**
- **Not every vulnerability report is actually a vulnerability**
  - Improper configuration
  - Oversight in analysis
  - Falsified information
- **It's important to differentiate between a vulnerability and the report of a vulnerability**
- **CERT/CC attempts to catalog all new reported vulnerabilities**



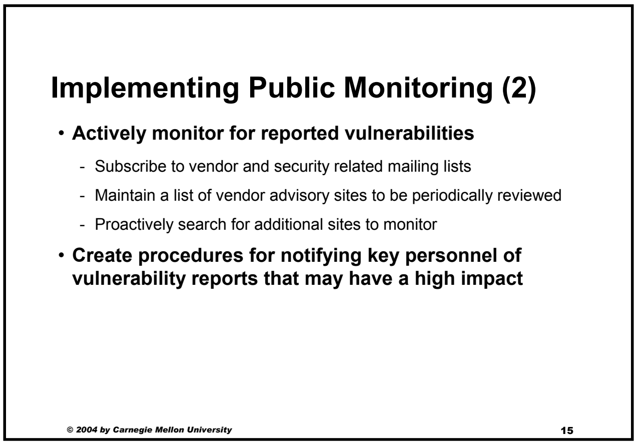
Step 3: Performing Surface Analysis

- **Public monitor discovers vulnerability report**
  - Do we have existing report?
- **Create a vulnerability report**
  - Unique ID, title, keywords, reporter contact information, URLs
- **Monitor for follow-up discussion**
  - Exploitation?
- **Vulnerability handler performs in depth analysis**
- **Public release of this information is coordinated by the CSIRT team**



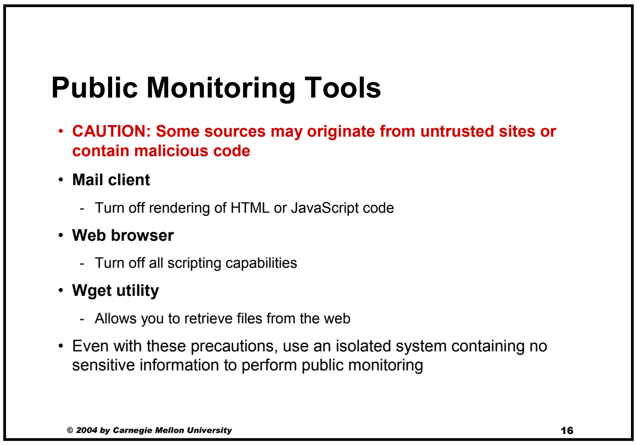
Implementing Public Monitoring

- **Utilize the three step process**
  - Identify information to be collected, identify and monitor sources of information, perform surface analysis
- **Train the public monitor**
  - Evaluate information quickly
  - Determine severity level of report
  - Proactively inform vulnerability handlers



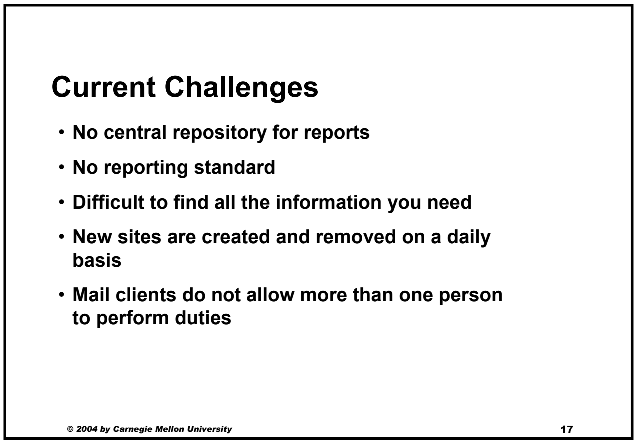
Implementing Public Monitoring (2)

- **Actively monitor for reported vulnerabilities**
  - Subscribe to vendor and security related mailing lists
  - Maintain a list of vendor advisory sites to be periodically reviewed
  - Proactively search for additional sites to monitor
- **Create procedures for notifying key personnel of vulnerability reports that may have a high impact**



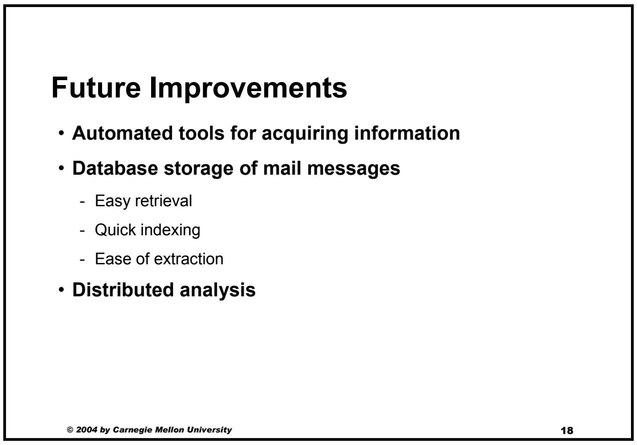
Public Monitoring Tools

- **CAUTION: Some sources may originate from untrusted sites or contain malicious code**
- **Mail client**
  - Turn off rendering of HTML or JavaScript code
- **Web browser**
  - Turn off all scripting capabilities
- **Wget utility**
  - Allows you to retrieve files from the web
- Even with these precautions, use an isolated system containing no sensitive information to perform public monitoring



Current Challenges

- **No central repository for reports**
- **No reporting standard**
- **Difficult to find all the information you need**
- **New sites are created and removed on a daily basis**
- **Mail clients do not allow more than one person to perform duties**



Future Improvements

- **Automated tools for acquiring information**
- **Database storage of mail messages**
  - Easy retrieval
  - Quick indexing
  - Ease of extraction
- **Distributed analysis**

Conclusion

- Role of the public monitor
  - Identify vulnerabilities, determine severity, provide informational awareness
- Utilize the three step process
  - Identify types of data to collect, identify and monitor sources of information, perform surface analysis
- How CERT/CC monitors
  - Tools, information sources, current limitations and future improvements

Useful Links

US-CERT
http://www.us-cert.gov

CERT/CC
http://www.cert.org

InfoSysSec
www.infosyssec.org

MARC
http://marc.theaimsgroup.com

Neohapsis
http://archives.neohapsis.com

OpenSource Vulnerability Database (OSVDB)
http://www.osvdb.org

Secunia
http://www.secunia.com

SecuriTeam
http://www.securiteam.com

SecurityFocus
http://www.securityfocus.com

SecurityTracker
http://www.securitytracker.com

Slashdot
http://www.slashdot.org

The Register
http://www.theregister.co.uk

Any suggestions for other sites/lists to actively monitor?

CERT® Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213
USA

Hotline: +1 412 268 7090 CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989

Web: http://www.cert.org/

Email: cert@cert.org