Leveraging the National Vulnerability Database

Tony Sager
Chief, Vulnerability Analysis & Operations Group
National Security Agency

Presentation to ACSAC - December 2006

VAO Mission

- *...identify, characterize, and put into operational context the* vulnerability *of the technology, information, and operations of the DoD and the national security community*
- *...help the community identify countermeasures, and start the path to solutions*

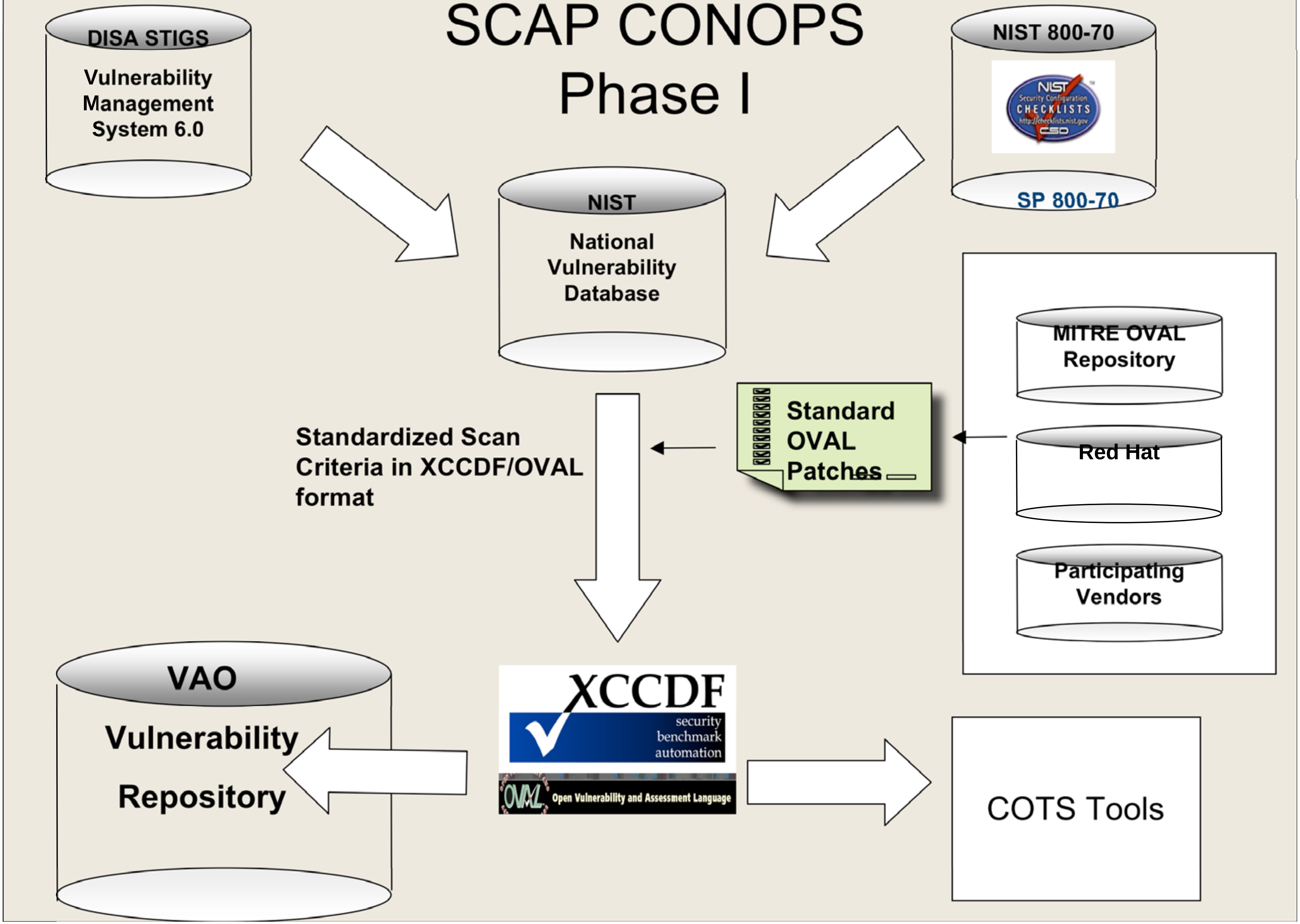
VAO Focus Areas

- Increase the sharing of vulnerability information
- Increase analysis to make sense of vulnerabilities

VAO Vulnerability Repository

- …a consolidation point of existing external security policy guidance and security automation related standards. Specifically:
    - SCAP
        - NVD
        - CVE, CCE (maybe), CPE, CVSS, etc.,…
        - XCCDF/OVAL
    - Internal – controlled NSA Security Guidance
    - Commercial Guidance
    - Data from Partners

SCAP CONOPS Phase I



DISA STIGS

Vulnerability Management System 6.0

NIST 800-70

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

SP 800-70

NIST

National Vulnerability Database

MITRE OVAL Repository

Red Hat

Participating Vendors

Standard OVAL Patches

Standardized Scan Criteria in XCCDF/OVAL format

XCCDF security benchmark automation
OVAL Open Vulnerability and Assessment Language

VAO

Vulnerability Repository

COTS Tools

Backup Slides

Security Content Automation Program (SCAP)

- Enables organizations to automate compliance, manage vulnerabilities and perform security measurement
- Content (XCCDF/OVAL) created under this program enable:
  - Vulnerability check to be mapped to high level compliance policies. These checklists automate all technical control compliance activities.
  - Organizations use the checklists to check for vulnerabilities (both mis-configurations and software flaws) and to measure their application security posture.
  - NIST recommends use of XCCDF/OVAL files to produce security control testing evidence within Federal Information Security Management Act (FISMA) compliance efforts.

Security Content Automation Program (SCAP)

- Security Guidance
  - Product vendors (Microsoft and Vista)
  - DISA – STIG & Platinum/Gold Disk
  - NSA Security Guides
  - NIST Special Publications
- XCCDF/OVAL content being created by:
  - Security Product vendors (Start-Ups)
    - Secure Elements, Threat Guard, others
    - NSA via MITRE. 3-4 month preliminary effort

Security Content Automation Program (SCAP)

- NSA sponsored XCCDF/OVAL content
  - Creating DoD specific content based on guidance from DISA STIG, Gold Disk, and NSA Security Guides. Content for:
    - Windows XP, Windows 2003 Server, Oracle 10g, Apache & Red Hat Linux