

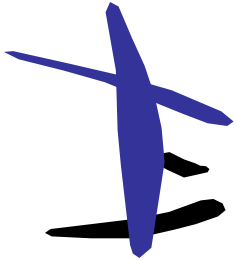


# Federal Desktop Core Configuration (FDCC)

---

Presented by: Saji Ranasinghe

Date: October, 2007



- **Federal Desktop Core Configuration (FDCC)**
  - Standardized Configuration with Hardened Security Settings to meet minimum functionality
  - Platform Specific
  - Based on existing guidelines
- **OMB Mandated**
  - OMB M-07-11 - Implementation of Commonly Accepted Security Configurations for Windows Operating Systems – March , 2007
  - OMB M-07-18 - Ensuring New Acquisitions Include Common Security Configurations – June, 2007
  - OMB Memo to CIOs - Establishment of Windows XP and Vista Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations – July, 2007
- **In Support of the OMB Mandate**
  - NIST Technical resources
  - MS Windows XP SP-2 and Vista FDCC Baseline Virtual Hard Disks
  - IE 7, Win XP Firewall and Vista Defender enabled
  - AD Group Policy Objects



## OMB Memo M-07-11

Win XP and Vista Clients when deployed need to be configured according to an approved and agreed upon common Security Configuration - Baseline

Submit Draft Implementation plans by May 1, 2007.

Adopt FDCC by February 1, 2008.

## OMB Memoranda



## OMB Memo for CIOs – July 31<sup>st</sup>, 2007

XP and Vista + IE 7 .VHD files with pre configured FDCC Security Settings to test, evaluate and certify applications by the vendors.

S-CAP validation tools for Agencies and Vendors to check FDCC compliance and certify applications.

## OMB Memo M-07-18

IT Providers shall certify their applications to be fully functional and operate correctly as intended in FDCC.

The approved FDCC configuration shall not be altered.

Applications designed for normal end users shall run in the standard user context.



- Common core Microsoft Windows configuration driven by OMB.
- Based on the DISA, NSA, NIST, USAF, and Microsoft existing guidelines for securing Windows XP and Vista. (Check Lists)
- Leverage USAF standard configuration Desktop initiative.
  - Successfully Deployed and tested across half a million Windows XP Systems.
- Include Security and other settings (Agencies are not required to use these settings)
  - Internet Explorer 7.
  - Firewall is enabled for Windows XP and Vista.
  - Windows Vista Defender is enabled.



# Microsoft Virtual PC - .VHD Files

---

- VPC and .VHD Files
  - Virtual PC
    - Allows users to run a virtual instance of an operating system
    - Free Download (Virtual PC 7.0)
  - Virtual Hard Disk Files (.VHD)
    - Virtual instance of an Operating System
    - Runs on the Host OS
    - Utilize the hardware of the computer (e.g., hard drive, Ethernet card, USB ports) in the same way the non-virtual
  - MS XP and MS Vista .VHD files are configured according to the FDCC Security Requirements



# Microsoft Virtual PC - .VHD Files

---

- Benefits of using .VHD Files
  - Test Production Applications before migrating for functionality issues.
  - Test applications during the SDLC phases.
  - Test Updates, Patches and their impact on the production environment before introducing them to the production environment.
  - VHDs can be discarded and reimplemented very quickly for the purposes of ensuring a pristine testing environment or if something malfunctioned with the previous VHD.
  - Multiple VHDs can be run over a single physical platform to achieve cost savings.



# SCAP (I)

---

- **SCAP**

- Method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).
- A selected suite of interoperable and automatable XML based standards.
- Method for cataloging software flaws, security related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements.
- Simultaneously machine and human readable.
- The National Vulnerability Database provides a repository and data feeds of content that utilize the SCAP standards.



# SCAP (II)

---

- Leverages six (6) open standards for creating SCAP content
- SCAP content consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations
- Benchmarking of the OS using predefined SCAP content





# SCAP (III)

---

- **Responsibilities of NIST**

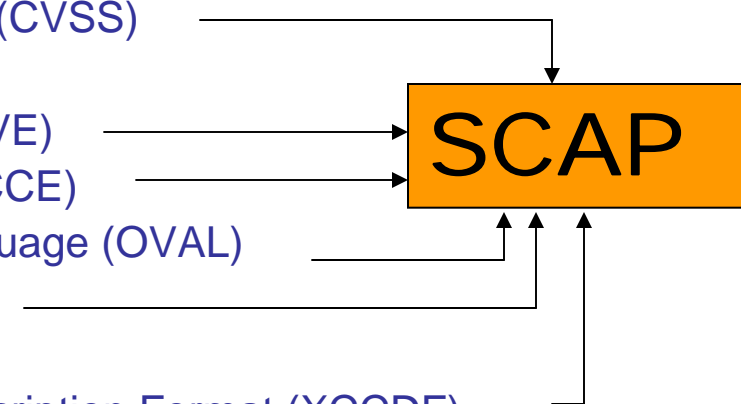
- Defines and maintains the protocol and the data feeds of content.
- Defines how to use the open standards within the SCAP context and defines the mappings between the SCAP enumeration standards.
- Check List Program reviews and approves submitted check lists by Federal Agencies and Vendors.
- Does not control the underlying standards that are used within the protocol.



# SCAP (IV)







## Combining Existing Initiatives

- **DISA**
  - STIG & Checklist Content
  - Gold Disk & VMS Research
- **FIRST**
  - Common Vulnerability Scoring System (CVSS)
- **MITRE**
  - Common Vulnerability Enumeration (CVE)
  - Common Configuration Enumeration (CCE)
  - Open Vulnerability & Assessment Language (OVAL)
  - Common Platform Enumeration (CCP)
- **NSA**
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Security Guidance & Content
- **NIST**
  - National Vulnerability Database
  - Checklist Program
  - Security Content Automation Program



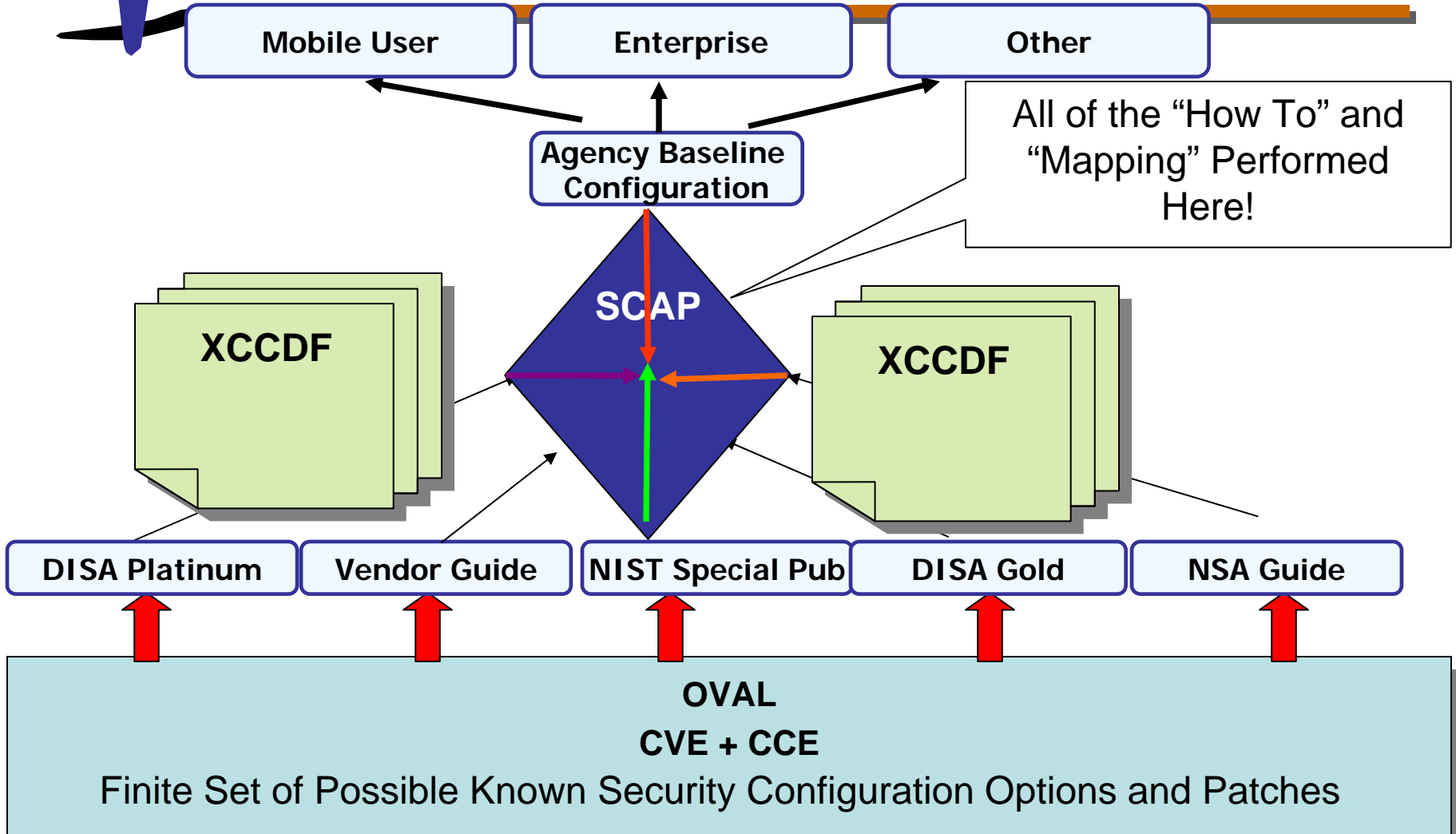


# SCAP (V)

 cve.mitre.org	<u><a href="#">CVE</a></u>	<b>Common Vulnerabilities and Exposures</b>	Standard identifiers and dictionary for security vulnerabilities related to software flaws
 cce.mitre.org	<u><a href="#">CCE</a></u>	<b>Common Configuration Enumeration</b>	Standard identifiers and dictionary for system configuration issues related to security
 cpe.mitre.org	<u><a href="#">CPE</a></u>	<b>Common Platform Enumeration</b>	Standard identifiers and dictionary for platform/product naming
 security benchmark automation	<u><a href="#">XCCDF</a></u>	<b>eXtensible Configuration Checklist Description Format</b>	Standard XML for specifying checklists and for reporting results of checklist evaluation
 oval.mitre.org	<u><a href="#">OVAL</a></u>	<b>Open Vulnerability and Assessment Language</b>	Standard XML for testing procedures for security related software flaws, configuration issues, and patches as well as for reporting the results of the tests
	<u><a href="#">CVSS</a></u>	<b>Common Vulnerability Scoring System</b>	Standard for conveying and scoring the impact of vulnerabilities



# SCAP (VI)





# SCAP

---

## Beta Security Automation Files Available

- Windows Vista
  - Misconfigurations
  - DISA/NSA/NIST, Microsoft, Air Force policies
- Windows XP
  - Misconfigurations/Software flaws
  - NIST FISMA and DISA policies (SP 800-68 / Gold Disk)
- Windows Server 2003
  - Misconfigurations/Software flaws
  - Microsoft and NIST FISMA policies
- Red Hat Enterprise Linux
  - Software flaws

Many more under development!!



# SCAP Tool Vendor Adoption

---

- Tool Vendor Adoption of SCAP

- ThreatGuard



- First product to perform automated compliance evaluation and remediation using SCAP

- Secure Elements



- Tenable Nessus (under development)

- Asserted Statements of Compliance to SCAP

- Symantec

- McAfee

- ASG

- ManTech

- CSC



# NIST Publications

---

- [NIST Checklist Publication \(Revised Special Publication 800-70\)](#)
- [NIST - Information Security Automation Program \(ISAP\)](#)
- [NIST IR 7275 – XCCDF version 1.1.2 \(Draft Posted\)](#)



# Objectives of SCAP

---

- Enable technical control compliance automation
  - Low level vulnerability checks to map to high level compliance requirements
- Enable standardized vulnerability management
  - Empower security product vendor community to perform on-demand, Government directed security and compliance audits
  - End user organization can specify requirements
  - COTS tools automatically perform checks
- Enable efficient security measurement
  - FISMA scorecard have a quantitative component that map to actual low level vulnerabilities

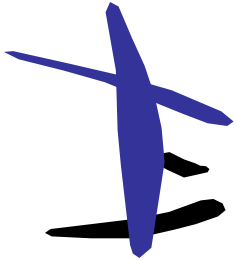




# Objectives (continued)

---

- Replace Stove-pipe GOTS Approaches
- Establish vulnerability management standards
- Encourage product vendors (i.e. Microsoft, Sun, Oracle, Red Hat etc.) to provide direct support in the form of security guidance/content



# Benefits of SCAP

---

## ■ Federal Agencies

- OMB is mandating Federal Agencies to move towards standardized common desktop configuration.
- Automation of technical control compliance (FISMA).
- Ability of agencies to specify how systems are to be secured.
- Ability to measure security using standardized methods.

## ■ COTS Tool Vendors

- Vendors compete on quality of tool, not the checking content .
- Provision of an enhanced IT security data repository.
  - No cost and license free.
  - Standards based: CVE/OVAL/XCCDF/CVSS/CCE.
  - Cover both software flaw and configuration issues.
- Elimination of duplication of effort/cost reduction through standardization.

## ● Security Configuration Management made easier



# Resources

---

- [NIST FDCC](#)
- [NIST SCAP](#)
- [NVD CVE/CCE data feed](#)
- [CVE Homepage](#)
- [CCE Homepage](#)
- [CPE Homepage](#)
- [CVSS Homepage](#)
- [XCCDF Standard](#)
- [OVAL Homepage](#)