Secure Desktop Configurations under FDCC

CONFIGURING FOR SUCCESS

Prepared by:

Nabil Ghadiali

Electrosoft

11417 Sunset Hills Road, Suite 228
Reston, VA – 20190
Tel: (703)-437-9451 Fax: (703)-437-9452
http://www.electrosoft-inc.com

November 2007

PART-I: INTRODUCTION

Over the past decade, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the National Institutes for Standards and Technology (NIST) have all published hardening guidance for various operating systems and applications.

The NSA guidance hasn't been considered a formal standard, but rather actionable advice to help Department of Defense (DoD) agencies improve their information system security posture. DISA has been publishing Security Technical Implementation Guides (STIG) and checklists that define requirements for DoD agencies to follow when deploying information technology. Similarly, NIST has also written special publications for securing various platforms and applications that many civilian agencies meticulously apply as NIST's recommended configuration settings. Finally, there is the Microsoft Solutions for Security and Compliance (MSSC) team that is responsible for providing security configuration guides for MS Operating Systems.

The main goal of these efforts was to improve the security of the computers and networks used by federal agencies, but unfortunately in many instances there were contradictory advice provided between these agencies as well as from other sources of guidance that are available today.

In 2003 the US Air Force (USAF) identified enhanced configuration management as a key goal for reducing the cost of managing computers running Windows. Working with Microsoft Consulting Services their IT team developed a single configuration for all of the Air Force. The cost savings were significant!

The success at the USAF caught the eye of officials at the Office of Management and Budget (OMB), inspiring a memorandum to be sent out from OMB directing all federal agencies to develop plans for deploying a standard desktop configuration.

GOVERNANCE

OMB M-07-11: ***Implementation of Commonly Accepted Security Configurations for Windows Operating Systems***
Web URL: - http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf

OMB M-07-18: ***Ensuring New Acquisitions Include Common Security Configurations***
Web URL: - http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf

FDCC MEMO: ***Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations***
Web URL: - http://cio.gov/documents/FDCC_memo.pdf

FEDERAL DESKTOP CORE CONFIGURATION

The Federal Desktop Core Configuration (FDCC) is a security configuration that was the outcome of the OMB Memoranda M-07-11.

The FDCC currently exists for Microsoft Windows Vista and XP operating systems.

EFFECT ON AGENCIES

Based on OMB M-07-11, Agencies are requested to submit their draft implementation plans by May 1, 2007. Additionally, agencies with either of the above mentioned operating systems and/or plans to upgrade to these operating systems have to adopt these standard security configurations by February 1, 2008.

OMB Memoranda M-07-18 provides recommended language for agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations.

WHAT AGENCIES NEED TO THINK ABOUT!

Having secure and standardized configurations for all operating systems irrespective of it being a workstation or server is fundamental to an agency's security and configuration management policy.

However in the context of FDDC and OMB Memo M-07-11, Agencies need to adopt this standard only for their Windows XP and Vista operating system environments by the deadline of February 1, 2008.

In order to meet this mandate, here are some questions that need to be addressed:

- Which operating systems are currently in use and what are the configurations for each?

- Is there a standard configuration that is applied as part of the Agency CM policy based on the OS?
- Is there a plan for upgrading to either Windows XP or Vista? If yes, what is the number of IT Systems that will be affected?
- Is there a standard set of applications that are installed on each system? If the same set is not installed, how many different configurations are present?
- Is there a known set of roles and is there a finite set of privileges that apply to the usage of the IT system associated with each role (e.g. Admin, User etc.)
- Has it been determined that the applications typically installed in the agency's computing environment run correctly in this secure configuration mode ? Has this information been obtained from the vendor and/or has it been tested?
- Based on these applications, has the agency determined that a deviation from the FDCC configuration settings is necessary or not?

The above-mentioned list is not intended to be exhaustive, but merely throw light on the fact that certain activities need to be thought through by the OCIO and agency IT Managers to make sure that they are positioned to meet the mandate's deadline.

Please contact Electrosoft at info@electrosoft-inc.com to learn more about how Electrosoft can support your Agency to comply with OMB M-07-11.

PART-II: THE TECHNICAL DETAILS

THE INFORMATION SECURITY AUTOMATION PROGRAM

The Information Security Automation Program (ISAP) is a U.S. government multi-agency initiative to enable automation and standardization of technical security operations. ISAP is being formalized through a trilateral memorandum of agreement (MOA) between Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST). The Office of Secretary of Defense (OSD) also participates and the Department of Homeland Security (DHS) funds the operation infrastructure on which ISAP relies (i.e., the National Vulnerability Database).

The ISAP high level objective includes standards based automation of security checking and remediation as well as automation of technical compliance activities (e.g. FISMA). ISAP's low level objectives include enabling standards based communication of vulnerability data, customizing and managing configuration baselines for various IT products, assessing information systems and reporting compliance status, using standard metrics to weight and aggregate potential vulnerability impact, and remediating identified vulnerabilities.

ISAP's technical specifications are contained in the related Security Content Automation Protocol (SCAP).

SCAP

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance).

SCAP is a suite of selected open standards that enumerate 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 in order to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined. The National Vulnerability Database provides a repository and data feeds of content that utilize the SCAP standards.

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.

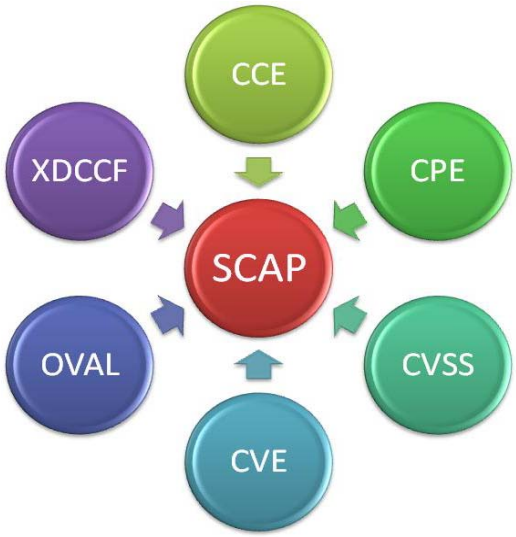

Figure 1 - SCAP Standards

The SCAP security checklist data is configuration checklists written in machine readable languages (XCCDF). They conform to an SCAP template and style guide to ensure compatibility with SCAP products and services. SCAP checklists reference SCAP test procedures.

The SCAP enumerations are a list of all known security related software flaws (CVE), a list of known software configuration issues (CCE), and a list of standard vendor and product names (CPE).

SCAP is comprised of the following standards:

Common Vulnerabilities and Exposures (CVE): - is a list or dictionary that provides common identifiers for publicly known information security vulnerabilities and exposures. CVE is managed by The MITRE Corporation and is sponsored by the U.S. Department of Homeland Security.
Web URL - http://cve.mitre.org/

Common Configuration Enumeration (CCE): - provides common identifiers to system configurations in order to facilitate fast and accurate correlation of configuration data. Within SCAP, CCE is primarily used to identify security related

configuration issues. CCE is managed by The MITRE Corporation and is sponsored by the U.S. Department of Defense.
Web URL - http://cce.mitre.org/

Common Platform Enumeration (CPE): - is a structured naming scheme for information technology systems, software, and packages. It is simply a standards based dictionary of software product names (e.g., vendor names, product names, version numbers, and editions). CPE is managed by The MITRE Corporation and is sponsored by the U.S. Department of Defense.
Web URL - http://cpe.mitre.org/

Common Vulnerability Scoring System (CVSS): - is an open standard for assigning scores to a vulnerability that indicates its relative severity compared to other vulnerabilities. CVSS is managed by the Forum of Incident Response and Security Teams (FIRST)
Web URL - http://www.first.org/cvss/index.html

Extensible Configuration Checklist Description Format (XCCDF): - is a specification language for writing security checklists, benchmarks and other configuration guidance. Development of the XCCDF specification is being led by the U.S. National Security Agency, published by the U.S. National Institute of Standards and Technology (NIST), and developed with contributions from the security community.
Web URL - http://nvd.nist.gov/xccdf.cfm

Open Vulnerability and Assessment Language (OVAL): - is the common language for security experts to discuss and agree upon technical details about how to check for the presence of vulnerabilities on computer systems. This XML-based language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. OVAL is managed by The MITRE Corporation and is sponsored by the U.S. Department of Homeland Security
Web URL - http://oval.mitre.org/

FDCC Details

For those of you who are interested in knowing where the details for the FDCC-based configuration settings were established - here is some information!

The Windows Vista FDCC is based on DoD customization of the Microsoft Security Guides for both Windows Vista and Internet Explorer 7.0. Microsoft's Vista Security Guide was produced through a collaborative effort with DISA, NSA, and NIST. The guide reflects the consensus recommended settings from DISA, NSA, and NIST for the Windows Vista platform.

The Windows XP FDCC is based on Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST SP 800-68 and DoD customization of the recommendations in Microsoft's Security Guide for Internet Explorer 7.0

So, how does an agency check compliance of their information technology systems to this new configuration standard? Further, how do you determine whether your applications can execute correctly within this new secure settings - the answer - VHD images.

FDCC Compliance Testing

NIST and the Department of Homeland Security are working with Microsoft to establish a virtual machine to provide agencies and information technology providers' access to Windows XP and VISTA images.

By using Virtual PC (VPC), a Microsoft product that allows users to run a virtual instance of an operating system (i.e. Virtual Hard Disk) within an already running instance of an operating system, agencies can very quickly test and evaluate whether their applications are operating correctly.

The Virtual Hard Disk (VHD) can utilize the hardware of the computer (e.g., hard drive, Ethernet card, USB ports) in the same way the actual OS does. These VHD images are pre-configured with the recommended security settings based on FDCC. Agency software can be installed on a VHD in the same way software is installed on normal operating systems, whether their applications operate correctly under a particular set of security configurations.

Advantage of using these VHDs is that they can be discarded and reimplemented very quickly for the purposes of ensuring a pristine testing environment or if something malfunctioned with the previous VHD. Additionally, multiple VHDs can be run over a single physical platform.

FDCC SCAP content in VHDs is available for Windows XP and Vista at: http://csrc.nist.gov/fdcc/download_fdcc002Ehtml. The National Vulnerability Database (NVD) hosts all SCAP reference data, inclusive of profiles for the FDCC and other Windows XP and Windows Vista security configurations.

As SCAP content develops for the different operating systems, agencies will be able to easily verify compliance of configurations of their operating systems to these standards using SCAP-compliant tools.

FDCC AND FISMA

The VHD images developed at NIST are accurately calibrated to represent and test compliance with the FDCC recommendations.

Agencies can acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST's SCAP to help evaluate providers' self-assertions.

Furthermore, through the use of SCAP compliant tools and official FDCC SCAP content, agencies can routinely monitor their systems to ensure that the FDCC settings have not been altered as the result of patching, installation of new software, or human interaction. The tools compare the deployed configuration against the official SCAP FDCC content and report on any discrepancies so that corrective action can be taken (some tools also have an automatic remediation capability).

Finally, by way of this, Departments and agencies can automate much of their FISMA technical security control compliance activities by regularly scanning their computer systems using these SCAP checklists as well. The SCAP checklists have FISMA compliance mappings embedded within the checklist so that SCAP-compatible tools can automatically generate NIST Special Publication 800-53 assessment and compliance evidence. Each security configuration check is mapped to the appropriate NIST SP 800-53 security control.

The FDCC SCAP content also contains mappings to other high level policies (e.g., ISO, DOD 8500, FISCAM) and SCAP tools may also output those compliance mappings.

REFERENCES

[1] - http://nvd.nist.gov/scap.cfm

[2] - http://fdcc.nist.gov/

[3] - http://blogs.technet.com/fdcc/