FEDTECH

[Bridging the Gap]

Connecting the Dots

NIST develops an automated approach to help agencies make the jump from security policies and mandates to secure systems.

By Stephen D. Quinn

Establishing traceability from the Federal Information Security Management Act's high-level requirements down to specific mechanisms to secure hardware and software poses challenges for the government's systems security managers.

Effectively using security controls hinges on ensuring that an agency's technology staff can properly establish and enforce their systems' security configuration settings. At the National Institute of Standards and Technology, we continue to look for ways to help agencies do that.

To make this important linkage from law and policy to the mandatory security requirements and controls described in Federal Information Processing Standard 200 and NIST Special Publication 800-53 — and ultimately to the mechanisms at the systems-implementation level — NIST established the Security Content Automation Program. SCAP is part of the NIST FISMA Implementation Project, now in Phase II, and the agency's Information Security Automation Program.

Through the interagency ISAP effort, the government — in cooperation with academia and industry — encourages widespread support for the SCAP, a suite of open standards that provide technical specifications for expressing and exchanging security-related data. These interoperable standards — developed primarily by the National Security Agency, Mitre and NIST — identify, enumerate, assign and facilitate the measurement and sharing of information-security-relevant data.

The SCAP suite likely will expand over time to include additional standards, such as Common Remediation Enumeration and Open Vulnerability Remediation Language.

How It Works

The primary output from SCAPare security checklists in a standard eXtensible Markup Language format that agencies (and vendors) can use via automated commercial products to help build, operate, measure and maintain secure systems according to official government security recommendations. Each security checklist contains instructions for configuring information technology products for an operational environment or verifying that an information technology product has already been securely configured.

The checklists can take many forms, including files that can automatically set or verify security configurations. Having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, executive orders, directives, policies, regulations, standards and guidance. Another need for such lists arises from the

RELATED MOST POPULAR

Tools of the Trade
With the right technology, best practices and people power, CISOs say they can keep federal systems and data secure.

Before They Arrive
Don't ask when or if a breach will occur. Instead, ask yourself: Has the IT team set the stage to stop and contain an intrusion?

The X Factor
Women find mind and mission align in government tech jobs. What's the takeaway that agencies can capitalize on to help maintain a skilled federal IT workforce?

The IT Chief's New Clothes
What penetration testing and vulnerability scans will and won't do, and how they might fit into your agency's security program.

Beyond the Flash
Government takes aim at a wireless future with HSPD-12 ID cards.

Do More Than Report About IT Security
OMB has created the Information Systems Security Line of Business to expedite partnering on common solutions.

8 Tips to Keep Data Safe
From around the globe to around the block, here's help securing your systems.

Protect Your Digital Assets
Recent data thefts are just the tip of an ugly iceberg, but it's not too late to slow down and build a better foundation for data security.

Making the Grade
What does it take to earn a passing mark on the IT security report card? Check out our primer to help your agency improve its efforts.

Privacy Matters
Privacy goes part and parcel with security: Get some pointers on the new FISMA templates for detailing your agency's privacy projects.

increasing number of vulnerabilities in systems and the growing sophistication of threats against those vulnerabilities.

Help From Everywhere

Because of these needs, the SCAP team encourages development of automated checklists within government and by industry and academic institutions. In particular, it's seeking lists compliant or compatible with eXtensible Checklist Configuration Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL).

These are widely used for automated checklists — XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL for mapping high-level technical checks to the low-level details of executing those checks on the operating systems or applications being assessed.

The SCAP Web site, at nvd.nist.gov/scap.cfm, provides automated security configuration and patching information in a standard format for the following checklists: Microsoft Windows Vista, 2003 Server and XP; Office 2007; Internet Explorer 7.0; Symantec AntiVirus; and Red Hat Linux. While NIST is working with vendors to translate the checklist content for other popular operating systems and applications — including Sun Solaris; Netscape Navigator and other versions of Office; Oracle and Microsoft SQL Server databases; and Web servers such as IIS and Apache — the English prose version of these and other security checklists can be found at checklists.nist.gov.

Through automation, agencies can ensure they consistently apply security controls and configuration settings within their systems and know that they have a mechanism for effectively verifying those controls and settings.

Fact

June 30, 2007 The date when agencies buying products that run Microsoft Windows Vista or XP must ensure these products conform to recommended security settings on the NIST Checklist Web site. Agencies can use the SCAP content to automatically test, implement and report compliance with the recommended checklist configuration controls.

Focusing the Government's I.T. Security Resources

The Information Security Automation Program (ISAP) is a Homeland Security Department-sponsored initiative that includes interagency participation by the National Institute of Standards and Technology, National Security Agency and Defense Information Systems Agency. This program focuses on a standard, automated approach for the implementation of systems security controls to achieve the following objectives:

- **Develop** requirements for automated sharing of information security data;
- **Customize** and manage configuration baselines for IT products;
- **Assess** information systems, and report compliance status;
- **Use** standard metrics to weigh and aggregate potential vulnerability impact;
- **Remediate** identified vulnerabilities.

Recognizing that NIST has the responsibility to produce security configuration guidance for the government and that NSA and DISA provide a similar service to the Defense Department, the ISAP governing program consolidates data resources from these agencies and provides them in a standardized SCAP eXtensible Markup Language format. The SCAP files contain information about:

- **Checking** for security-related software flaws and misconfigurations;
- **Mapping** to higher-level policies, such as the Federal Information Security Management Act of 2002 via NIST Special Publication 800-53 or the DOD 8500 information assurance directive;
- **Providing** a standard impact metric for vulnerabilities and a capability to aggregate impact scores at the agency-reporting level.

SCAP's Component Standards

Enumeration
Common Platform Enumeration — CPE
Common Vulnerability Enumeration — CVE (NIST SP 800-51)
Common Configuration Enumeration — CCE

Metrics & Scoring
Common Vulnerability Scoring System — CVSS

Expression Languages
eXtensible Checklist Configuration Description Format (XCCDF; NIST Interagency Report 7275)
Open Vulnerability and Assessment Language (OVAL)

For more information about NIST's Information Security Automation Program and Security Content Automation Program, visit nvd.nist.gov/scap.cfm.

Stephen D. Quinn, a senior computer scientist at the National Institute of Standards and Technology, is program manager of the interagency Information Security Automation Program and co-originator of the Security Content Automation Protocol.

[Related Articles]

- Tools of the Trade
- Before They Arrive
- The X Factor
- The IT Chief's New Clothes
- Beyond the Flash
- Do More Than Report About IT Security
- 8 Tips to Keep Data Safe
- Protect Your Digital Assets
- Making the Grade
- Privacy Matters

[Bridging the Gap]

Connecting the Dots

NIST develops an automated approach to help agencies make the jump from security policies and mandates to secure systems.

By Stephen D. Quinn

Establishing traceability from the Federal Information Security Management Act's high-level requirements down to specific mechanisms to secure hardware and software poses challenges for the government's systems security managers.

Effectively using security controls hinges on ensuring that an agency's technology staff can properly establish and enforce their systems' security configuration settings. At the National Institute of Standards and Technology, we continue to look for ways to help agencies do that.

To make this important linkage from law and policy to the mandatory security requirements and controls described in Federal Information Processing Standard 200 and NIST Special Publication 800-53 — and ultimately to the mechanisms at the systems-implementation level — NIST established the Security Content Automation Program. SCAP is part of the NIST FISMA Implementation Project, now in Phase II, and the agency's Information Security Automation Program.

Through the interagency ISAP effort, the government — in cooperation with academia and industry — encourages widespread support for the SCAP, a suite of open standards that provide technical specifications for expressing and exchanging security-related data. These interoperable standards — developed primarily by the National Security Agency, Mitre and NIST — identify, enumerate, assign and facilitate the measurement and sharing of information-security-relevant data.

The SCAP suite likely will expand over time to include additional standards, such as Common Remediation Enumeration and Open Vulnerability Remediation Language.

How It Works

The primary output from SCAPare security checklists in a standard eXtensible Markup Language format that agencies (and vendors) can use via automated commercial products to help build, operate, measure and maintain secure systems according to official government security recommendations. Each security checklist contains instructions for configuring information technology products for an operational environment or verifying that an information technology product has already been securely configured.

The checklists can take many forms, including files that can automatically set or verify security configurations. Having such automated methods has become increasingly important for several reasons, including the complexity of achieving compliance with various laws, executive orders, directives, policies, regulations, standards and guidance. Another need for such lists arises from the

RELATED MOST POPULAR

Tools of the Trade
With the right technology, best practices and people power, CISOs say they can keep federal systems and data secure.

Before They Arrive
Don't ask when or if a breach will occur. Instead, ask yourself: Has the IT team set the stage to stop and contain an intrusion?

The X Factor
Women find mind and mission align in government tech jobs. What's the takeaway that agencies can capitalize on to help maintain a skilled federal IT workforce?

The IT Chief's New Clothes
What penetration testing and vulnerability scans will and won't do, and how they might fit into your agency's security program.

Beyond the Flash
Government takes aim at a wireless future with HSPD-12 ID cards.

Do More Than Report About IT Security
OMB has created the Information Systems Security Line of Business to expedite partnering on common solutions.

8 Tips to Keep Data Safe
From around the globe to around the block, here's help securing your systems.

Protect Your Digital Assets
Recent data thefts are just the tip of an ugly iceberg, but it's not too late to slow down and build a better foundation for data security.

Making the Grade
What does it take to earn a passing mark on the IT security report card? Check out our primer to help your agency improve its efforts.

Privacy Matters
Privacy goes part and parcel with security: Get some pointers on the new FISMA templates for detailing your agency's privacy projects.

increasing number of vulnerabilities in systems and the growing sophistication of threats against those vulnerabilities.

Help From Everywhere

Because of these needs, the SCAP team encourages development of automated checklists within government and by industry and academic institutions. In particular, it's seeking lists compliant or compatible with eXtensible Checklist Configuration Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL).

These are widely used for automated checklists — XCCDF primarily for mapping policies and other sets of requirements to high-level technical checks, and OVAL for mapping high-level technical checks to the low-level details of executing those checks on the operating systems or applications being assessed.

The SCAP Web site, at nvd.nist.gov/scap.cfm, provides automated security configuration and patching information in a standard format for the following checklists: Microsoft Windows Vista, 2003 Server and XP; Office 2007; Internet Explorer 7.0; Symantec AntiVirus; and Red Hat Linux. While NIST is working with vendors to translate the checklist content for other popular operating systems and applications — including Sun Solaris; Netscape Navigator and other versions of Office; Oracle and Microsoft SQL Server databases; and Web servers such as IIS and Apache — the English prose version of these and other security checklists can be found at checklists.nist.gov.

Through automation, agencies can ensure they consistently apply security controls and configuration settings within their systems and know that they have a mechanism for effectively verifying those controls and settings.

Fact

June 30, 2007 The date when agencies buying products that run Microsoft Windows Vista or XP must ensure these products conform to recommended security settings on the NIST Checklist Web site. Agencies can use the SCAP content to automatically test, implement and report compliance with the recommended checklist configuration controls.

Focusing the Government's I.T. Security Resources

The Information Security Automation Program (ISAP) is a Homeland Security Department-sponsored initiative that includes interagency participation by the National Institute of Standards and Technology, National Security Agency and Defense Information Systems Agency. This program focuses on a standard, automated approach for the implementation of systems security controls to achieve the following objectives:

- **Develop** requirements for automated sharing of information security data;
- **Customize** and manage configuration baselines for IT products;
- **Assess** information systems, and report compliance status;
- **Use** standard metrics to weigh and aggregate potential vulnerability impact;
- **Remediate** identified vulnerabilities.

Recognizing that NIST has the responsibility to produce security configuration guidance for the government and that NSA and DISA provide a similar service to the Defense Department, the ISAP governing program consolidates data resources from these agencies and provides them in a standardized SCAP eXtensible Markup Language format. The SCAP files contain information about:

- **Checking** for security-related software flaws and misconfigurations;
- **Mapping** to higher-level policies, such as the Federal Information Security Management Act of 2002 via NIST Special Publication 800-53 or the DOD 8500 information assurance directive;
- **Providing** a standard impact metric for vulnerabilities and a capability to aggregate impact scores at the agency-reporting level.

SCAP's Component Standards

Enumeration
Common Platform Enumeration — CPE
Common Vulnerability Enumeration — CVE (NIST SP 800-51)
Common Configuration Enumeration — CCE

Metrics & Scoring
Common Vulnerability Scoring System — CVSS

Expression Languages
eXtensible Checklist Configuration Description Format (XCCDF; NIST Interagency Report 7275)
Open Vulnerability and Assessment Language (OVAL)

For more information about NIST's Information Security Automation Program and Security Content Automation Program, visit nvd.nist.gov/scap.cfm.

Stephen D. Quinn, a senior computer scientist at the National Institute of Standards and Technology, is program manager of the interagency Information Security Automation Program and co-originator of the Security Content Automation Protocol.

[Related Articles]

- Tools of the Trade
- Before They Arrive
- The X Factor
- The IT Chief's New Clothes
- Beyond the Flash
- Do More Than Report About IT Security
- 8 Tips to Keep Data Safe
- Protect Your Digital Assets
- Making the Grade
- Privacy Matters

» comment | » print | » email | del.icio.us | digg this | reddit | rss feeds

Home | Contact Us | About Us | Subscribe | Meet The Editors | Privacy | Site Map | Terms and Conditions