Panel Discussion – Examples of Successful Integration of Tools into Software Assurance

Facilitator: Michael Kass, NIST

Mini-Keynote: Jon Stevenson, Veracode

Software Assurance Forum

5 November, 2009

TTPE Working Group Background

- Technology, Tools and Product Evaluation (TTPE) Working Group Goal:
  - To assist in bringing software assurance tools and technologies into the government's effort to improve the speed and accuracy of software assurance evaluation and certification of COTS, GOTS and open source software.

Some TTPE Objectives

- Specify dictionaries for low-level descriptions of software weakness (CWE), attack patterns and terminology (CAPEC)
- Measure the assurance tool functionality and capability of SwA tools through SAMATE (SATE)
- Support development of OMG Software Assurance Ecosystem Specifications
- The Software Assurance Findings Expression Schema (SAFES)
- Software Assurance Landscape Document

Panel Goals

- Help answer questions
  - Where are we in software assurance?
  - Where are we going?
  - What challenges do we face?
  - What suggestions do we have for the SwA Forum?

Our Panel

- Mini-Keynote: Jon Stevenson, Veracode
- Panelists:
  - David Waltermire, NIST
  - John Streufert, State Department
  - Jim Chen, UMUC
  - Andras Szakal, IBM

David Waltermire, NIST

- David Waltermire is an IT specialist at the National Institute of Standards and Technology (NIST).
- He is the specification architect for the Security Automation Program and has been a significant contributor to the Security Content Automation Protocol (SCAP).
- Dave also oversees the NIST National Checklist Program. Prior to joining NIST, Dave worked as a security consultant with Booz Allen Hamilton were he focused on the advancement of security automation capabilities.
- During his 14 year career, he has worked as a systems and network administrator with a focus on operational security and as a software engineer pioneering the first standards-based configuration assessment tool.

John Streufert, State Department

- John Streufert joined the Department of State team in July 2006 as the Chief Information Security Officer and Deputy Chief Information Officer for Information Security.
- Since arriving at State he lowered a material weakness on IT Security to a deficiency and raised the IT Security grade from an F to a B as assessed by OMB and Congress.
- In July 2008 at Mr. Streufert’s request, the Department began providing letter grades monthly to executives and technical managers on progress in lowering IT security risk based on correcting scanned vulnerabilities and configuration weaknesses.
- This program resulted in the reduction of 89% of the measured risk in 12 months enterprise-wide with a security metrics program administered by a coalition of 11 technical organizations.
- Mr. Streufert was a graduate of the Maxwell School of Public Administration, Syracuse University (MPA) in 1985 and St. Olaf College (B.A.) in 1979

Jim Chen, UMUC

- Dr. Chen is Professor and Program Director of Information Assurance in the Department of Information and Technology Systems in the Graduate School of Management & Technology at the University of Maryland University College.
- The Information Assurance Specialization that he manages is designated by the NSA and the DHS as one of the National Centers of Academic Excellence in Information Assurance Education. He is also in charge of the Network Systems and Security Laboratory.
- Dr. Chen has been teaching graduate courses in network and Internet security, intrusion detection band intrusion prevention, computer and network forensics, data communications, telecommunications, networking, network management, and Internet technologies.

Andras Szakal, IBM

- IBM Distinguished Engineer and Chief Architect of IBM's Federal Software business unit.
- Open Group Distinguished Certified IT Archtiect, IBM Certified Service Oriented Architecture (SOA) Solution Designer and a Certified Secure Software Lifecycle Professional (CSSLP).
- His responsibilities include developing e-Government software architectures using IBM middleware and leading the IBM U.S. Federal Software IT Architect Team.
- He holds undergraduate degrees in Biology and Computer Science and a Masters Degree in Computer Science from James Madison University.

Jon Stevenson, Veracode

- Senior Vice President of Technology and Service Operations at Veracode
- Responsible for all aspects of engineering, product management, security research and service delivery as well as managing Veracode’s closed-loop continuous improvement process and overall quality of service.
- Jon brings over 25 years of experience leading large R&D organizations with both Engineering and Product Management responsibility.
- Jon holds a BS in mechanical engineering from the University of Delaware and an MS degree in mechanical engineering from California State University at Long Beach.

Software Security Simplified

VERACODE

Veracode Goals as a Stakeholder

Provide a simple and cost-effective way to accurately identify and manage application security risk

CVS/pharmacy® for all the ways you care™

DTCC

KAISER PERMANENTE®

BlueCross BlueShield of Alabama

FAMILY DOLLAR

Experian™ A world of insight

BARCLAYS

McAfee®

First Data™

DELTA

FEDERAL AVIATION ADMINISTRATION

The Washington Post

Today's growing security problem

- The software industry is the world's largest manufacturing industry ($235B) with NO notion of security quality. It forms the fabric of our modern infrastructure.
- 7,000 new security vulnerabilities in 2007 and over $117B in losses from identity theft alone…and things are getting worse.

2007

America's Hackable Backbone Researchers hack into and take control over a nuclear power plant

2007

iPhone hacked in minutes after launch; multiple vulnerabilities found, Apple discloses backdoor "feature" on iPhone

2007

Experimental cyber attack causes generator to self-destruct. Could cause $700B in damage on mass scale

2008

FAA announces New Boeing 787 plane controls could be taken over by hackers during flight

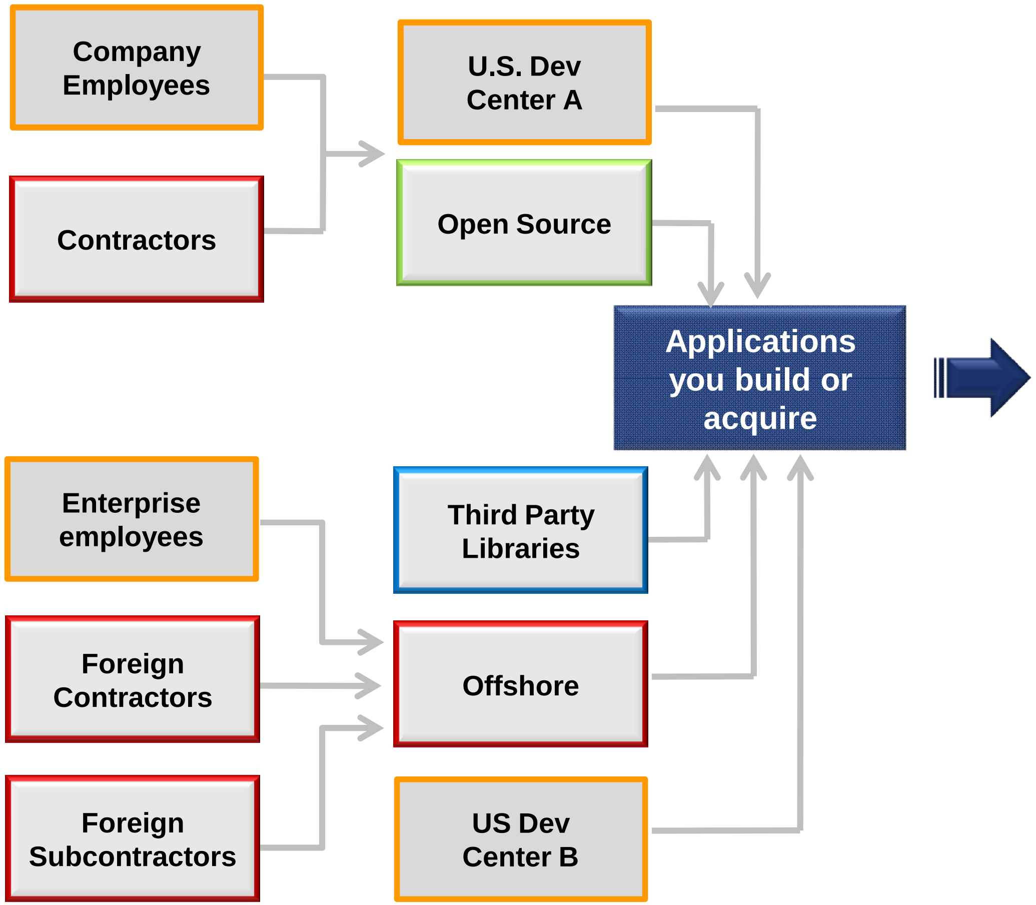
2008

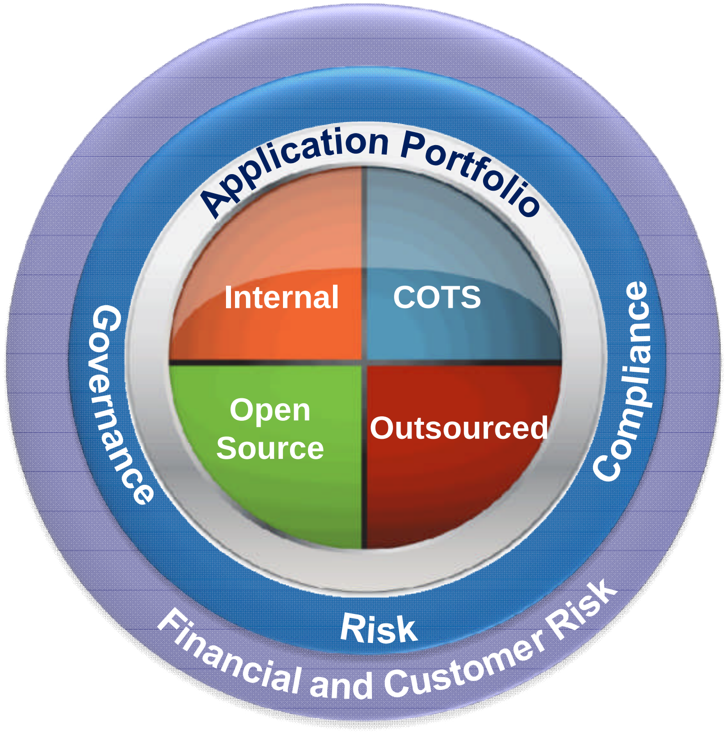
Multiple cross-site scripting (XSS) vulnerabilities discovered in Google, Facebook and MySpace. Backdoors found in Gmail

2009

SQL Injection vulnerabilities at Heartland Financial, Hannaford and 7-11 lead to data breaches resulting in the theft of over 130 million credit cards.

Why are applications hard to protect?



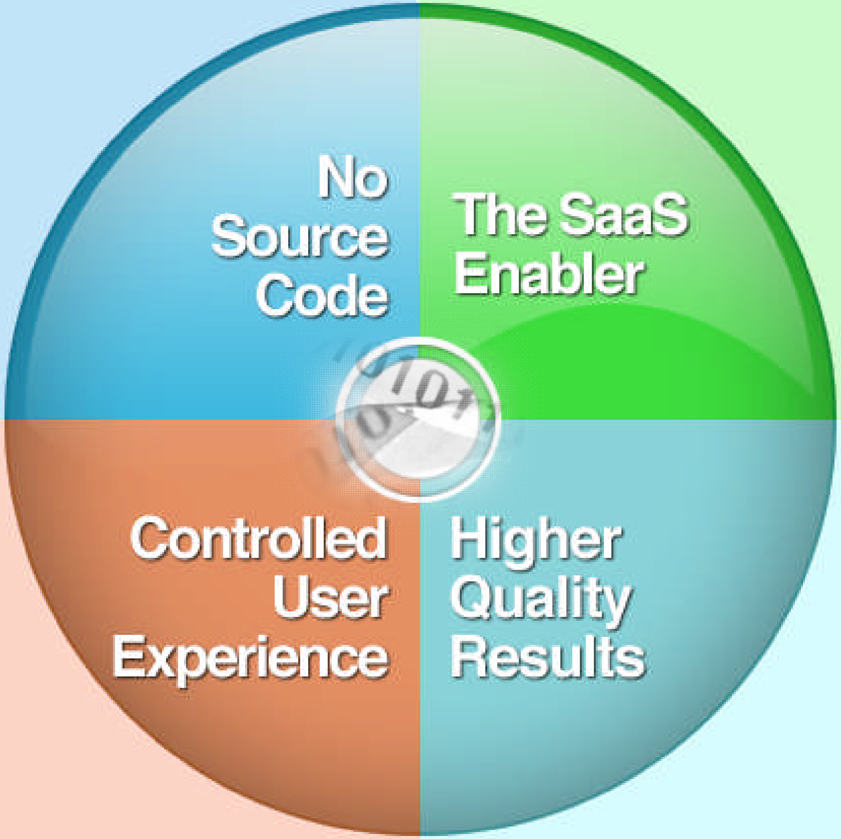


Software of Unknown Pedigree (SOUP)

Solution: binary application analysis

- Independent
- Removes 3rd party testing objections
- Unlocks multiple use cases (COTS, Outsourcing, M&A)

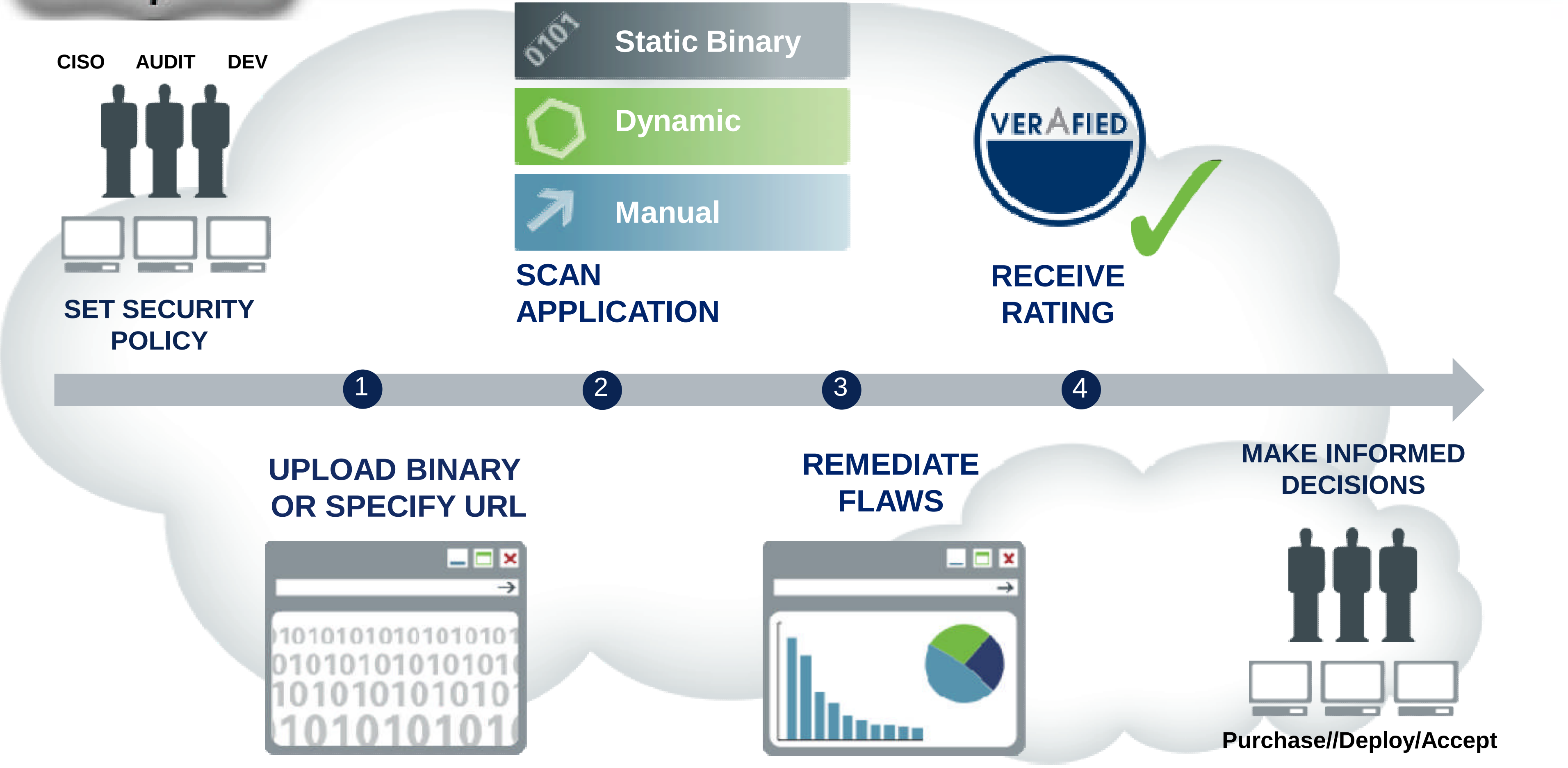
- Enables global reach & scale
- Serves entire supply chain
- Drives automation



- Designed for non-security professionals
- Makes it easy for mass market consumption

- Über-Security Audit
- Scans for backdoors, tool configuration issues, & security features
- Industry’s lowest false positive rates

What Veracode does today



CISO AUDIT DEV

SET SECURITY POLICY

1 UPLOAD BINARY OR SPECIFY URL

2 SCAN APPLICATION

- Static Binary
- Dynamic
- Manual

3 REMEDIATE FLAWS

4 RECEIVE RATING

MAKE INFORMED DECISIONS

Purchase//Deploy/Accept

What can the DHS forum do?

- Define common format for consumption of discovered vulnerabilities
- Sponsor a lab to compare coverage and accuracy of available security tools
- Promote language mandating independent assessment and verification of application security
- Promote independent rating of software security
- Promote certification of software developers

Thank You

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

NIST
Security Automation

David Waltermire

david.waltermire@nist.gov

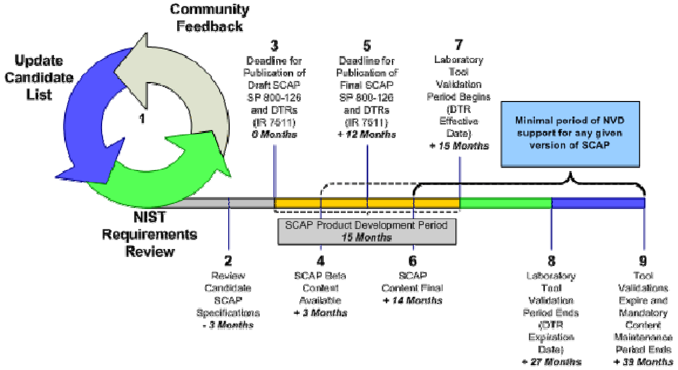
Homeland Security

NIST Security Automation Goals

- **Minimize Effort:** Reduce the time and effort of manual assessment and remediation/mitigation
- **Advance Interoperability:** Provide standardized communication and automation methods
- **Improve Situational Awareness:** Enable fast and accurate correlation within the enterprise and across organizations/agencies
- **Increase Transparency:** Make content more transparent
    - What/How to check
    - What was found (Results)
- **Economy of Scale:** SCAP security content can be developed once, with use by many

Current State

- Fully functional, broadly tested security automation protocol with applicability in vulnerability and technical compliance management
- High level benefits of interoperability, repeatability, uniform decision material, uniform reporting format
- Self-documenting compliance
- Predictable product validation lifecycle


Community Feedback
Update Candidate List
1
NIST Requirements Review
3 Deadline for Publication of Draft SCAP SP 800-126 and DTRs (IR 7511) 0 Months
5 Deadline for Publication of Final SCAP SP 800-126 and DTRs (IR 7511) + 12 Months
7 Laboratory Tool Validation Period Begins (DTR Effective Date) + 15 Months
Minimal period of NVD support for any given version of SCAP
SCAP Product Development Period 15 Months
2 Review Candidate SCAP Specifications - 3 Months
4 SCAP Beta Content Available + 3 Months
6 SCAP Content Final + 14 Months
8 Laboratory Tool Validation Period Ends (DTR Expiration Date) + 27 Months
9 Tool Validations Expire and Mandatory Content Maintenance Period Ends + 39 Months

- Currently delivers:
  - Repeatable assessments and uniform reporting - OMB's FDCC
  - Standardized software flaw and impact measurement - PCI DSS v1.2
  - 17 SCAP-expressed checklists – National Checklist Program

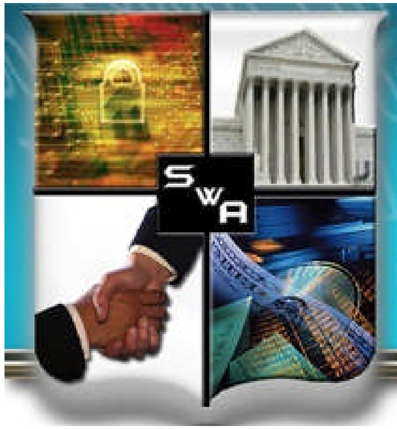
Challenges

We need to:

- Establish automation capabilities to allow remediation and mitigation of software flaws and mis-configurations
- Enable human interaction to assess operational and managerial controls
- Expand SCAP to support trusted content and reporting aggregation
- Provide tools and capabilities to better support automation content creation
- Expand and integrate automation capabilities across additional security domains and functions
- Provide additional measures and metrics

What you can do…

- IT Vendors
  - Produce checklists in SCAP and submit to National Checklist Program
  - Produce CPE, CCE, and CVE’s for IT products
- Produce vulnerability alerts using SCAP
- Buy and use SCAP Validated products.
- Engagement and feedback
- Innovate



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Improving Software Assurance Education in IA Programs

Dr. Jim Q. Chen, Ph.D.

Professor and Program Director of Information Assurance

University of Maryland University College

University of Maryland University College

- Discussion Outline
  - Goals
  - Current status
  - Challenges
  - Solutions

Goals of SwA Education in IA Programs

- Raise the awareness of SwA
- Integrate SwA contents in academic curricula
- Provide students with relevant hands-on work experience
- Conduct research in SwA
- Produce highly qualified students

Current Status of SwA Education in IA Programs

- Not sufficiently emphasized
- Not adequately covered in academic curricula
- Not enough hands-on practical SwA projects and internships
- Not enough research in SwA
- Not enough graduates who are well-prepared to handle SwA

Challenges for SwA Education

- Gaps between goals and reality at the SwA awareness level
- Gaps between goals and reality during the SwA education process
- Gaps between goals and reality at the SwA product level

Essential Components in SwA Education

- Body of knowledge
- Domain expertise
- Hands-on practical experience

Solutions in Improving SwA Education

- Increase SwA awareness by introducing it at the beginning of an IA program
- Integrate SwA contents in academic curricula by providing a dedicated course or a set of dedicated courses on SwA
- Seek support from industry and government in providing students with unclassified hands-on practical projects, capstone projects, and internships
- Create community interest in conducting researches in SwA
- Create an environment that produces highly qualified students

Examples of Specific Tactics in SwA Education

- Discuss enterprise architecture
- Include SwA at the beginning of and throughout the life cycle
- Emphasize good design and good programming practice
- Evaluate, test, and modify design and programming products
- Show the limitations of patches and add-ons

A New Approach in Teaching SwA

- Teach the basics of SwA in the first course of the IA specialization: INFA610 Computer Security, Software Assurance, Hardware Assurance, and Security Management
- Have the lab exercises related to software assurance in other INFA courses
- Teach a SwA-focused course in INFA670 Information Assurance Capstone

Network Systems and Security Laboratory

- Designed and set up a remote-access Network Systems and Security Laboratory
- Designed and developed various types of lab exercises for students
  - Remote-access lab exercises
  - Simulated lab exercises
  - Off-line lab exercises

Intellectual Merits of the Lab

- The challenges for students
  - Solve real-life problems
  - Go beyond the textbooks
  - Work in teams in virtual environment
- The use of open-source software
  - Develop extra plug-ins and rules for Snort, an open-source software-based intrusion detection and intrusion prevention system
  - Save substantial cost in using the open-source solutions such as VMware ESXi server, VMware Server, Snort, WireShark, etc.
- The use of virtual platforms
  - Easy to manage and maintain
  - Easy to use multiple operating systems in one environment
- The easy access for learners
- The promotion of innovative design

Example Topics Covered in a SwA Course

- Building systems with assurance
- Secure software development lifecycle
- Secure software design and secure construction
- Secure software verification, validation, and evaluation
- Secure software tools and methods
- Secure software project management
- Secure software sustainment and acquiring secure software

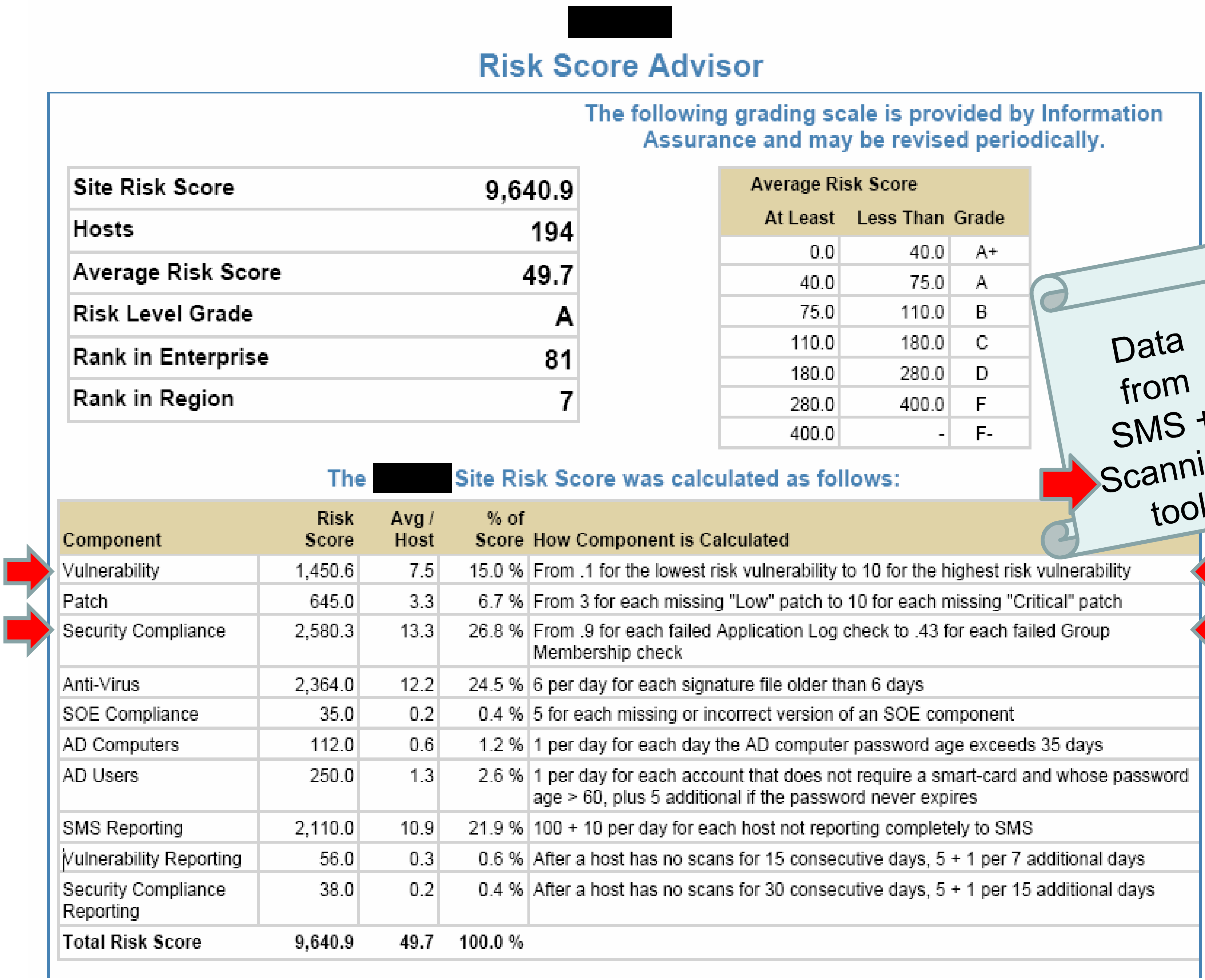
- Unclassified SwA case studies and real-life scenarios
- Unclassified SwA topics for hands-on practical projects and capstone projects
- Internships

Implementation of the Consensus Audit Guidelines

John Streufert, CIO, U.S. State Department

Software Assurance Forum

5 November, 2009



[redacted]

Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	9,640.9
Hosts	194
Average Risk Score	49.7
Risk Level Grade	A
Rank in Enterprise	81
Rank in Region	7

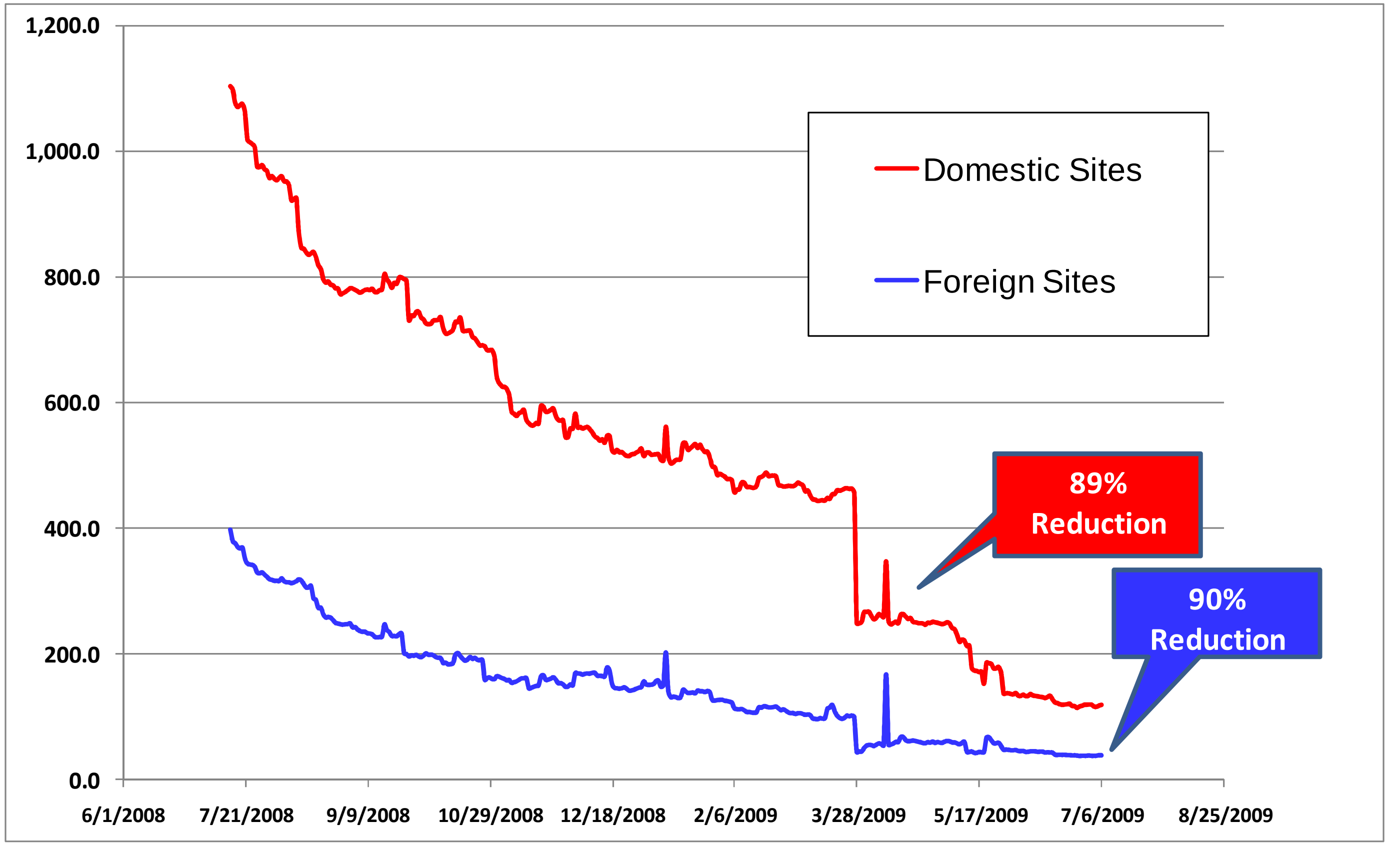
Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

The [redacted] Site Risk Score was calculated as follows:

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
Vulnerability	1,450.6	7.5	15.0 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch	645.0	3.3	6.7 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance	2,580.3	13.3	26.8 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
Anti-Virus	2,364.0	12.2	24.5 %	6 per day for each signature file older than 6 days
SOE Compliance	35.0	0.2	0.4 %	5 for each missing or incorrect version of an SOE component
AD Computers	112.0	0.6	1.2 %	1 per day for each day the AD computer password age exceeds 35 days
AD Users	250.0	1.3	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS Reporting	2,110.0	10.9	21.9 %	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting	56.0	0.3	0.6 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
Security Compliance Reporting	38.0	0.2	0.4 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**9,640.9**	**49.7**	**100.0 %**	

Data from SMS + Scanning tool

Results in 12 Months



89% Reduction

90% Reduction

Attack Based Metrics Pilot

CAG ID	Consensus Audit Guidelines	NIST-800-53	CIRT Events 11 mo
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	Multiple Tools < 6% < 22%
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	
3	Secure configurations for HW and SW, if available	CM-6, CM-7, CP-10, IA-5, SC-7	Nominal
4	Secure configurations for network devices such as firewalls and routers	AC-4, CM-6, CM-7, CP-10, IA-5, RA-5, SC-7	Nominal
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	< 7%
6	Maintenance/Analysis of complete security audit logs	AU-1, AU-2, AU-3, AU-4, AU-6, AU-7, AU-9, AU-11, AU-12, CM-3, CM-5, CM-6, SI-4	Nominal
7	Application software security	AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11, SI-3	Decentralized
8	Controlled use of Administrative Privileges	AC-6, AC-17, AT-2, AU-2	Nominal
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	< 1%
10	Continuous vulnerability testing and remediation	CA-2, CA-6, CA-7, RA-5, SI-2	Nominal
11	Dormant account monitoring and control	AC-2, PS-4, PS-5	Nominal
12	Anti-malware defenses	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	< 60%
13	Limitation and control of ports, protocols and services	AC-4, CM-6, CM-7, SC-7	Not yet graded
14	Wireless device control	AC-17	Nominal
15	Data leakage protection	AC-2, AC-4, PL-4, SC-7, SC-31, SI-4	Pending

IBM as a Stakeholder in the Software Assurance Community
Andras R. Szakal, IBM Distinguished Engineer

- Goals as a Stakeholder in Assurance Community
  - Protect the client and the company
  - World class secure development practices and technologies
  - Champion open industry standards
- What are we doing to meet these goals
  - IBM Secure Engineering
  - Lead vendor approach to supply chain management & security
  - Research and Development focused on new assurance technologies
  - Participation in ICASI and IT-ISAC
  - Contribute to federal work groups

- What Challenges do we Face?
  - Federal community can be very inwardly focused
  - Lack of focus on risk management and balance with needs of the business
  - Unwillingness to embrace open international standards before seeking to create industry specific or agency level standards
  - Lack of understanding of how open source is managed and it’s value back to the COTS vendor community
    - who funds OSS
    - how is it managed

- What more can the DHS SwA Forum do?
  - Lean more about how global vendors manage their supply chain
  - Directly support the development of open industry standards
    - Learn more about ACE
    - Support CCMDB based solutions
    - Open could computing standards (DMTF, Open Group, etc).
  - Security as Architecture
  - CKI Security Architecture Best Practices