

SwA Fall 2012 Forum Agenda (as of September 17, 2012)

Theme: Measuring and Managing Risk From Software

MITRE-1, 7525 Colshire Drive, McLean, VA 22102

18 September (Tuesday) 8:00 AM –Registration 8:30 AM –Welcome and Overview 9:00 – 10:45 AM Opening Session 1	19 September (Wednesday) 8:00 AM –Registration 8:30 AM –Welcome and Overview 9:00 – 10:45 AM Opening Session 1	20 September (Thursday) 8:00 AM –Registration 8:30 AM –Welcome and Overview 9:00 – 10:45 AM Opening Session 1
TOWARD A RESILIENT CYBER ECOSYSTEM <i>Keynote –Michael Locatis, DHS Assistant Secretary for Cyber Security and Communications, DHS</i>	CAPABILITIES FOR STRENGTHENING CYBERSECURITY RESILIENCE IN THE HOMELAND SECURITY ENTERPRISE <i>Keynote – Dr. Peter Fonash, DHS</i>	<i>Keynote – Capers Jones</i>
TRUSTED AUTOMATED EXCHANGE OF INDICATOR INFORMATION (TAXII) • Richard Struse, DHS	<i>Panel on Understanding Risk through Software Assurance</i> • Richard Soley, OMG • Djenana Campara, KDM Analytics • Nancy Mead, SEI • Bob Martin, MITRE • Sean Barnum, MITRE	CASE STUDIES IN MANAGING RISKS FROM SOFTWARE <i>Directions for Effective Product Security Assessment</i> • Eric Baize, SAFECODE
Morning Break	Morning Break	Morning Break
11:00 AM – 1 PM Session 2	11:00 AM – 1 PM Session 2	11:00 AM – 1 PM Session 2
CONTINUOUS MONITORING VIA SOFTWARE ASSURANCE AUTOMATION <i>Overview</i> • Bob Martin, MITRE <i>Monitoring for Threats & Attacks</i> • Sean Barnum, MITRE <i>Cyberpatterns</i> • Clive Blackwell, Oxford, UK	<i>Bringing Trust to Applications with Hardware-based Security</i> • Rick Doten, DMI <i>Common Software Weaknesses Reported in Electronic Voting Systems</i> • Mike Kass & Joshua Franklin, NIST <i>Implementing Software Assurance & the Application Software Assurance Center of Excellence (ASACoE), Process</i> • MSgt William P. Tooke, ASACoE	CASE STUDIES IN MANAGING RISKS FROM SOFTWARE <i>Recognizing and Responding to the Insider Threat</i> • Clive Blackwell, Oxford, UK <i>Collaborative Research Into Threats (CRITs)</i> • Matt Richard, MITRE. <i>National Initiative for Cybersecurity Education</i> • Peggy Maxson, DHS
Lunch Break	Lunch Break	Lunch Break
1:30 – 3:15 PM Session 3	1:30 – 3:15 PM Session 3	1:30 – 3:15 PM Session 3
CONTINUOUS MONITORING VIA SOFTWARE ASSURANCE AUTOMATION <i>Monitoring Assurance of Software</i> • Bob Martin, MITRE <i>Metrics - The Next Frontier</i> • Mark Wireman, OpenSky <i>Monitoring for Malware</i> • Ivan Kirillov, MITRE	MANAGING RISKS THROUGH SOFTWARE ASSURANCE <i>On Measurement</i> • Dan Geer, In-Q-Tel <i>Automating Architectural Analysis for Software Risk Management</i> • Lev Lesokhin, CAST <i>How Auditing and Metrics Contribute to making Secure Software</i> • Steve Winterfeld, TASC	EMERGING INITIATIVES IN MANAGING RISKS FROM SOFTWARE <i>NSF's Secure and Trustworthy Cyberspace (SaTC) program</i> • Jeremy Epstein, NSF <i>Emerging Initiatives from DHS</i> • Kevin E. Greene, DHS S&T
Afternoon Break	Afternoon Break	Afternoon Break
3:30 – 5 PM Session 4	3:30 – 5 PM Session 4	3:30 – 5 PM Session 4
<i>Choosing the Right Software Assurance Tool</i> • Paul Black, NIST	MANAGING RISKS THROUGH SOFTWARE ASSURANCE <i>Third Party Application Risk Program</i> • Chris Wysopal, Veracode, <i>Panel on Outsourced Third Party Assessments</i> • Chris Wysopal, Vericode • Keesha Crosby, HP Fortify/ Versatech • Penny Parkinson, Cigital <i>DOD Mini SOAR updates</i> • Don Davidson, DoD	EMERGING INITIATIVES IN MANAGING RISKS FROM SOFTWARE <i>Creating Self Defending Applications to Repel Attackers</i> • Michael Coates, OWASP <i>The Hyperion System: Computing Software Behavior with Function Extraction Technology</i> • Rick Linger ORNL <i>Getting off the 'X'</i> • Roger Hockenberry, CIA
5:00 – 5:30 PM Wrap-Up Outbrief	5:00 – 5:30 PM Wrap-Up Outbrief	5:00 – 5:30 PM Wrap-Up Outbrief -

18 September (Tuesday)

TOWARD A RESILIENT CYBER ECOSYSTEM

Michael W. Locatis, Assistant Secretary for Cyber Security and Communications, Department of Homeland Security (DHS), Keynote Speech

Just like natural ecosystems, a resilient cyber ecosystem is made up of a lot of organisms, in this case the cyber enterprises of institutions, agencies, and other partners. These, in turn, consist of a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and devices (computers, software, and communications technologies) – that interact for multiple purposes. As outlined in the Quadrennial Homeland Security Review, our enterprise approach to risk reduction focuses on collective effort and shared responsibilities for a secure cyber ecosystem. DHS has developed a number of complementary, integrated information sharing initiatives to facilitate collaborative response and awareness. We engage with the private sector on a voluntary basis to provide onsite analysis, mitigation support, and assessment assistance.

TRUSTED AUTOMATED EXCHANGE OF INDICATOR INFORMATION (TAXII)

Richard Struse, DHS

TAXII - the Trusted, Automated eXchange of Indicator Information - is a set of technical specifications, documentation and resources set up to advance the detection, prevention and mitigation of cyber threats at "machine speed." The TAXII effort defines a set of services and exchange messages for communicating threat intelligence using the Structured Threat Information eXpression (STIX) in order to empower diverse types of organizations to easily choose what information to share and which partners to share it with. The ultimate goal of TAXII is to allow any organization's identification and analysis of suspicious activity to inform preventive measures for the broader community as rapidly as possible, forcing the adversary to expend significantly greater resources to avoid detection. TAXII builds upon multiple standardization initiatives developed in collaboration with the private sector under the sponsorship of DHS's Software Assurance (SwA) Program, including the Structured Threat Information eXpression (STIX), the Cyber Observable eXpression (CybOX) and the Malware Attribute Enumeration and Characterization (MAEC).

CONTINUOUS MONITORING VIA SOFTWARE ASSURANCE AUTOMATION

Bob Martin and Sean Barnum, MITRE

The DHS Software Assurance (SwA) program works collaboratively with federal government and private sector partners to provide resources, tools and information to reduce the number of exploitable weaknesses in software. The SwA program sponsors—via funding and tasking through MITRE—the enumerations, languages and schemas that enable cost-effective SwA automation.

Clive Blackwell, Oxford Brookes University, Cyberpatterns

In CAPEC (Common Attack Pattern Enumeration and Classification), attack patterns are structured textual descriptions of high-level attacks in terms of their characteristics and methods of exploitation. They use a top-down approach to catalog attacks and identify their key elements from the attacker's perspective, which is crucial to understanding attack motivation and methodology, such as with the Advanced Persistent Threat. Conversely, there is the bottom-up approach using pattern matching of observable events. However, we need to go beyond simple pattern matching using keywords and regular expressions, as adversaries often evolve their methods more quickly than the defense, to avoid detection. We can gather and correlate evidence from multiple sources to

identify related events that could be attack indicators, possibly using the CybOX (Cyber Observable eXpression) schema. This aids better situational awareness by matching related observable events with potential attack templates in a more systematic and structured way than simple pattern matching.

Mark Wireman, OpenSky, Metrics - The Next Frontier

The challenge that many decision makers are faced with is related to the questions: "What does that vulnerability mean to me in terms of risk?" and "What is the risk being assumed with the application?" Many scanning products are getting more proficient at identifying vulnerabilities and weaknesses, however, this is leaving Managers with piles of reports and no solid grasp of what to do with them, how to prioritize them, and how to resource for them. They know that, while the vulnerabilities and weaknesses may exist, the applications have yet to be compromised so not all vulnerabilities should be treated equally. This presentation offers a contextual view of putting the vulnerabilities within context, allowing for a prioritization based on actual Risk vs a specific vulnerability rating. It takes an approach that puts the vulnerabilities within context from the application's view, providing a metric that is then equated to an actionable entity, thereby driving clear resource decisions, as well as providing an answer to the question "What is the overall risk of the application?".

CHOOSING THE RIGHT SOFTWARE ASSURANCE TOOLS

Paul Black, NIST

The Center for Assured Software's (CAS) [Static Analysis Tool Study - Methodology](#) report defines evaluation and scoring of static analysis software assurance (SwA) tools along with measures, such as precision, recall, and discrimination, and how CAS used their publicly available [Juliet 1.1 test suite](#) in their study. The NIST [Software Assurance Metrics And Tool Evaluation \(SAMATE\)](#) team proposed a basic set and future code complexities for the Common Weakness Enumeration (CWE) Compatibility and Effectiveness Program starting with CWE-121 Stack-based Buffer Overflow. This tutorial presents the use of the CAS methodology, consideration of other tool selection factors such as languages handled and extensions, and use of the SAMATE CWE-121 proposed set in assisting software developers or contractors in selecting SwA tools suitable for their process. In addition, this tutorial explains how SwA tools fit into the software development life cycle (SDLC) and where and how to efficiently introduce such tools. Finally, attendees will become familiar with other resources, such as the SAMATE [Reference Dataset \(SRD\)](#).

19 September (Wednesday)

CAPABILITIES FOR STRENGTHENING CYBERSECURITY RESILIENCE IN THE HOMELAND SECURITY ENTERPRISE

Dr. Peter M. Fonash, DHS, Keynote Speech

The resilient cyber ecosystem of the future will require cyber defenses that are proactive, not reactive. Moreover, these defenses – as appropriate – need to marshal automated collective action to protect, detect, respond and recover our cyber assets. This presentation will categorize cyber-attacks and propose a set of future cyber ecosystem capabilities to mitigate those attacks. The list of desired capabilities is not expected to change as a result of changes in threats, attack methods, technologies, and processes. This is because our approach is based on broad attack categories, not the specific technical details of those cyber-attacks that will change as technology evolves. Nevertheless, the cyber ecosystem capabilities must be able to adapt to support new environments, such as the global supply chain, cloud and mobile technologies.

PANEL ON UNDERSTANDING RISK THROUGH SOFTWARE ASSURANCE: WHAT ARE ORGANIZATIONS DOING TO UNDERSTAND THEIR SOFTWARE CHALLENGES?

In a distributed system with multiple diverse components, a decision-making entity needs to know how much it can trust the components that are creating and distributing critical data since attacks against networks can penetrate interconnected computer systems within milliseconds, exposing data and jeopardizing operations. Today, the few tools available to mitigate these attacks are becoming ineffective against the rapidly evolving threat and vulnerability landscape. For these reasons, stakeholders need to be able to understand the risk and to obtain confidence in the system's ability to execute trusted behavior only and withstand malicious attacks during operations. However, current risk management practices often do not consider assurance issues in an integrated way. This results in project stakeholders unknowingly accepting assurance risks that can leave open unintended and severe security issues. This problem is mostly due to:

1. A lack of transparency and traceability between high level security policy/requirement and system artifacts that implements them, and,
2. The ambiguity associated with the vulnerability/weakness space, including coverage, definitions and impact, making the risk assessment process ad-hoc at best .

Addressing these challenges is only possible through a set of tightly integrated standards, since a solution requires a range of tools and capabilities so as to function as a comprehensive and systematic security assurance system. This is the focus of OMG's systems assurance and interoperability standards, and will be the discussion point for the session.

- **Richard Soley, OMG**
- **Djenana Campara, KDM Analytics**
- **Nancy Mead, SEI**
- **Bob Martin, MITRE**
- **Sean Barnum, MITRE**

Rick Doten, DMI, Bringing Trust to Applications with Hardware-based Security

Hardware-based security is an unfortunately seldom-leveraged solution to protect our enterprises by bringing a root of trust for system, user identity, and encryption of data. By insuring that only authorized users authenticate using cryptological certificates stored in secure hardware chips of PCs, tablets, and phones, we can also provide more granular application control of data to increase privacy. The core of trusted computing already exists in most PC systems today. Many PC's include a dormant Trusted Platform Module (TPM) that can be activated to encrypt hard drives on the hardware level, provide controlled network access, and deliver measurements on boot process for unauthorized changes. With an abstraction layer called the Trusted Software Stack (TSS) specification, we can leverage this strong authentication into applications. We can also use this credential for data encryption that can't suffer a man-in-the-middle attack like SSL, while giving the opportunity to digitally sign data and documents. Further, we can utilize hardware measurements to provide a level of system trust, which we could use to dynamically alter application access and functionality based on that trust level. This presentation will provide an overview of these current and future application security capabilities, and how developers will soon be able to leverage hardware roots of trust to make more secure applications.

Mike Kass and Joshua Franklin, NIST, Common Software Weaknesses Reported in Electronic Voting Systems

Michael Kass and Joshua Franklin are members of the NIST team contributing to the development of the Voluntary Voting System Guidelines (VMSG) and tests for electronic voting systems. They will discuss the

architectures of electronic voting systems typically used in the U.S. today, and the kinds of software security weaknesses and vulnerabilities identified in independent security assessments of those systems. In particular, reported security vulnerability information is presented from the 2007 state-sponsored California Top to Bottom Review (TTBR) and Ohio EVEREST independent security assessments of electronic voting systems used in those states. The Common Weakness Enumeration (CWE) is used to discuss software weaknesses reported in those testing campaigns.

MSgt William P. Tooke, ASACoE, Implementing Software Assurance & the ASACoE Process

The Application Software Assurance Center of Excellence (ASACoE) is the Air Force's premiere Software Assurance practitioner. The ASACoE's mission is to foster security into the software development life cycle and software acquisitions through tools, techniques, education and training. Since its inception in 2007 the ASACoE has visited 240 Program Management Offices, assessed 909 applications and trained 1500 developers.

MANAGING RISKS FOR EFFECTIVE SOFTWARE ASSURANCE

Dan Geer, In-Q-Tel, On Measurement

The most important thing the Software Assurance Community can do is to ensure that there is no silent failure. This means instrumentation, it means well designed surveillance regimes, it means an attention to the kind of metrics that come out of an airplane's black box, it means keeping things simple enough that, well, there are fewer surprises, and it may mean changing how you think about how you make tradeoffs. Repeating Kernighan, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it. Because security is not composable (and may never be), be very careful where the code you reuse comes from. Every time I see a page larded up with more domains than I have fingers, I plan never to visit them again. I know you have to compete; I ask that you not end up in a race to the bottom.

Lev Lesokhin, CAST, Automating Architectural Analysis for Software Risk Management

We need a new generation of software measures that spans the boundaries of layers, languages, and their technology platforms to detect severe software risks. A recent example is the 'Propagation Risk Index' that measures the severity with which a violation of good architectural or coding practice can get propagated across the thread of a transaction from the user interface through the business logic to the database and back. This type of software analysis and measurement is critical for detecting and prioritizing the most insidious types of security, resiliency, and performance problems.

Steve Winterfeld, TASC, How Auditing and Metrics Contribute to Making Secure Software

If you can't measure it then it is not important. Many of us have heard this during our security career as we explain how Cybersecurity is important to our organization. This talk will cover how we can we develop more secure software by developing the right audit processes / metrics that support decisions at the technical, Return on Cyber Investment (ROCI) and senior leadership level.

Chris Wysopal, Veracode, Third party Application Risk Programs

"3rd party application risk programs" perform application security testing on software vendor built applications for their enterprise customers. Here are some of the stats: 64 Enterprises have participated in the 3rd party testing process, 1500+ rounds of analysis performed across 400+ vendors and 800+ applications. The most mature programs in terms of scans, policy, process and success are a top 10 global software vendor and a global

payment company. From there we see a large number of financial services and a number of Fortune 50 companies leading the way. Chris describes his methodology for "3rd party application risk program" in link to a [webinar](#) on the subject.

PANEL ON OUTSOURCED THIRD PARTY ASSESSMENTS

"Do it yourself" assessments are yielding to outsourced "3rd party application risk programs." What have those 3rd party application risk programs encountered when performing application security testing on software vendor-built applications for their enterprise customers? Are the top global software vendors and global payments companies fielding mature programs in terms of scans, policy, process and success? Are the third party assessment methodologies robust, effective, comparable, and consistent across this growing industry?

- **Chris Wysopal, Veracode**
- **Keesha Crosby, HP Fortify / Versatech**
- **Penny Parkinson, Cigital**

DOD MINI SOAR UPDATES

- **Don Davidson, DoD**

20 September (Thursday)

Capers Jones, Namcook Analytics LLC

Keynote Presentation.

CASE STUDIES IN MANAGING RISKS FROM SOFTWARE

Eric Baize, SAFECode, Directions for Effective Product Security Assessment

SAFECode members have made significant investments in meeting their customers' needs for software that is resilient to malicious attacks. This session will discuss SAFECode's perspectives on software resilience and on how customers can determine that a supplier has applied effective measures to assure the resilience of the software it delivers. In doing so, we will also discuss some realities of commercial software development that should form the basis for customer expectations.

Clive Blackwell, Oxford Brookes University, Recognizing and responding to the Insider Threat

The insider threat is an important and intractable problem. A systematic model for analyzing incidents is proposed using the conjunction of our multilayered architectural model and incident classification system. We investigate a case study of the insider threat from CERT, and examine how patterns may help us detect and respond to these potentially damaging incidents.

Matt Richard, MITRE ,Collaborative Research Into Threats (CRITs)

Abstract TBD.

Peggy Maxson, DHS, National Initiative for Cybersecurity Education (NICE)

Ms. Maxson will update the SwA Community on the status of the National Cybersecurity Workforce Framework, training catalogue mapping; as well as the National Institute for Cybersecurity Studies Portal.

EMERGING INITIATIVES IN MANAGING RISKS FROM SOFTWARE

Jeremy Epstein NSF, NSF's Secure and Trustworthy Cyberspace (SaTC) program

NSF's Secure and Trustworthy Cyberspace (SaTC) program is one of the largest research programs at NSF, and one of the largest cybersecurity grant programs in the country. With over \$70M/year in grants in FY13, SaTC covers a broad range of technical topics, as well as interdisciplinary connections in social and behavioral sciences, cybereconomics, cybersecurity education, and transition to practice. In this talk, Jeremy will give an overview of the SaTC program and the current solicitation for proposals. Deadlines for submissions vary by proposal type: medium proposals are due Nov 30, small and cybersecurity education are due Dec 14, and Frontier proposals are due January 30 2013.

Kevin E. Greene, DHS, Emerging Initiatives from DHS

DHS is committed to providing seed investments in advanced research and development activities that support national cyber security objectives and have the potential to create sustainable project communities. This is achieved in part by enabling broad adoption and participation by public and private-sectors. Included in these efforts are initiatives of great interest to the Software Assurance Community. The Software Assurance Marketplace (SWAMP) is committed to bringing a transformative change to the national software assurance landscape by providing continuous software assurance capabilities to researchers and developers. By providing Software Assurance (SWA) researchers, tool developers, tool users, and educators who train our workforce a suite of secure and dependable analysis services, SWAMP will reduce the number of vulnerabilities deployed in software. Researchers who develop new SWA tools and methodologies will use the repositories and cyber infrastructure offered by the SWAMP to improve their technologies and tools, while software developers and adopters will use the same services to hunt for vulnerabilities in their software. Educators will use these services to offer hands-on experience in SWA techniques to their students.

Michael Coates, OWASP, Creating Self Defending Applications to Repel Attackers

Unlike banks, critical infrastructure, or secured facilities, most critical web applications have very few capabilities to detect or defend against malicious behavior from users. Imagine if a real-world bank allowed anyone to continually guess the combination to the vault and never called the police against the attempted burglary. This scenario closely mirrors the reality of our critical applications - designed with security controls that provide no feedback from intrusion attempts, remain unmonitored, and allow malicious activity to continue indefinitely without a defensive response. Learn how web applications can integrate attack-aware technologies to detect and prevent custom application level attacks. This talk will cover the technical details of design and implementation, organizational support requirements, and integration into a secure development lifecycle. In addition, we will discuss tips and lessons-learned from real world implementations of attack aware software to understand impacts on risk and attack awareness.

Rick Linger, ORNL, The Hyperion System: Computing Software Behavior with Function Extraction Technology

It is important in cybersecurity analysis to understand all of the behavior of software, whether intended or unintended, benign or malicious. Oak Ridge National Laboratory is developing the Hyperion system which employs Function Extraction technology to compute the behavior of software with mathematical precision in all circumstances of use. The objective is to move from an uncertain understanding of software derived in human

SwA Fall 2012 Forum Agenda (as of September 17, 2012)

Theme: Measuring and Managing Risk From Software

MITRE-1, 7525 Colshire Drive, McLean, VA 22102

time scale to a precise understanding computed in machine time scale. This theory-based process operates on the functional semantics of software and is not subject to the limitations of traditional syntactic methods. Applications include software assurance, vulnerability discovery, and malware and anti-tamper analysis. Current projects include analysis of smart grid embedded software for security vulnerabilities.

Roger Hockenberry, CIA, Getting off the 'X'

The world of cyber is quickly becoming more sophisticated with a lower barrier of entry for potential actors and nation states to create complicated attacks against targets. In this talk, we will discuss how the standard implementation of security suites creates a static target that provides attackers a single vector, or attack plane. "Getting off the X" will discuss methods that are being developed to help vary attack surface, create a changing dynamic to defend against various types of attacks, and how the commercial world is looking to address these issues.