Security Measurement:

Supporting Information Needs for Securing Cyberspace

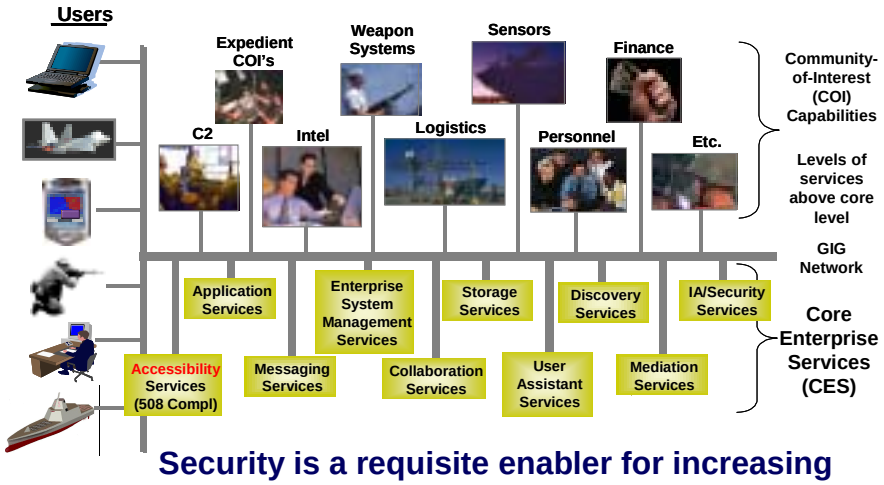
July 20, 2005

Homeland Security

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
US Department of Homeland Security

Net-Centric Enterprise Services

Support real-time & near-real-time warrior needs, and business users



Security is a requisite enabler for increasing reliance upon information -- ensure "trust"

Cyberspace & physical space are increasingly intertwined and software controlled/enabled

- **Chemical Industry**
  - 66,000 chemical plants

- **Banking and Finance**
  - 26,600 FDIC institutions
- **Agriculture and Food**
  - 1.9M farms
  - 87,000 food processing plants

- **Water**
  - 1,800 federal reservoirs
  - 1,600 treatment plants
- **Public Health**
  - 5,800 registered hospitals

- **Postal and Shipping**
  - 137M delivery sites
- **Transportation**
  - 120,000 miles of railroad
  - 590,000 highway bridges
  - 2M miles of pipeline
  - 300 ports

- **Telecomm**
  - 2B miles of cable
- **Energy**
  - 2,800 power plants
  - 300K production sites

- **Key Assets**
  - 104 nuclear power plants
  - 80K dams
  - 5,800 historic buildings
  - 3,000 government facilities
  - commercial facilities / 460 skyscrapers

Homeland Security

An Asymmetric Target-rich Environment

3

THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

February, 2003

"In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible."

President George W. Bush

Homeland Security

4

Driving Needs for Software Assurance

- Software vulnerabilities jeopardize intellectual property, business operations and services, infrastructure operations, and consumer trust
- Growing awareness and concern over the ability of an adversary to subvert the software supply chain
  - Federal Government relies on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements
  - Software development offers opportunities to insert malicious code and to poorly design and build software enabling exploitation
- Growing concern about inadequacies of suppliers' capabilities to build and deliver secure software with requisite levels of integrity
  - Current education & training provides too few practitioners with requisite competencies in secure software engineering
  - Concern about suppliers not exercising "minimum level of responsible practice"
  - Growing need to improve both the state-of-the-practice and the state-of-the-art on software capabilities of the nation
- Processes and technologies are required to build trust into software acquired and used by Government and critical infrastructure

Strengthen operational resiliency of software-enabled capabilities

Why Software Assurance is Critical

- Increasing awareness and acceptance of changing realities
  - Software is the core of system functionality
  - Global market & networked environment create opportunities & challenges
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software Size & Complexity (obscures intent and precludes exhaustive test)
  - Outsourcing and use of unvetted software supply chain (COTS & custom)
  - Attack sophistication (easing exploitation)
  - Reuse (unintended consequences increasing number of vulnerable targets)
  - Number of vulnerabilities and incidents
  - Number of threats targeting software
  - Risk of Asymmetric Attack and Threats

Software and the processes for acquiring and developing software represent significant weaknesses in attempts to secure cyberspace

Homeland Security

6

Software Assurance Program Overview

- Program based upon the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:

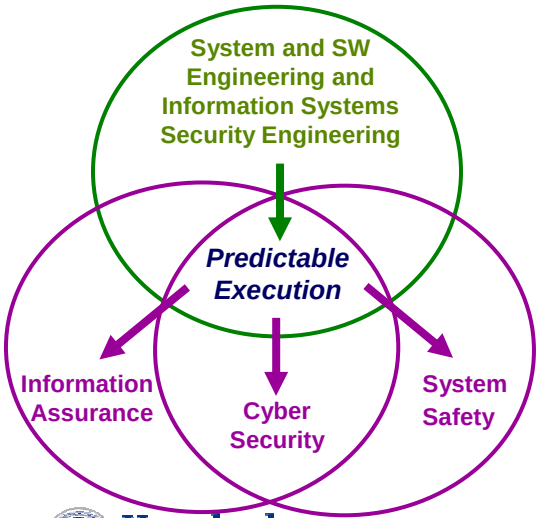
  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."

- DHS Program goals promote the security of software across the development life cycle
- Software Assurance (SwA) program is scoped to address software trustworthiness, predictable execution and conformance
  - Trustworthiness - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted
  - Predictable Execution - Justifiable confidence that software, when executed, functions in a manner in which it is intended
  - Conformance - Planned and systematic set of multi-disciplinary activities that ensure software processes and products conform to requirements, standards/procedures

Homeland Security

7

Relating SwA to Engineering Disciplines



For a safety/security analysis to be valid …

The execution of the system must be *predictable to enable resiliency*.

This requires …

- **Correct implementation of requirements, expectations and regulations.** — ***Traditional concern***
- **Exclusion of unwanted function even in the face of attempted exploitation.** — ***Growing concern***

Homeland Security

8

Software Assurance Program Structure

- Structured to facilitate public-private partnership, primarily relying on volunteer participation by industry, academia and government.
- Program framework encourages the production and acquisition of better quality and more secure software and leverages resources to target the following four areas:
  - People – developers (includes education and training) and users
  - Processes – best practices, standards, and practical guidelines for the development of secure software
  - Technology – software evaluation tools and diagnostic capabilities
  - Acquisition – software security improvements through specifications and guidelines for acquisition and outsourcing

Homeland Security

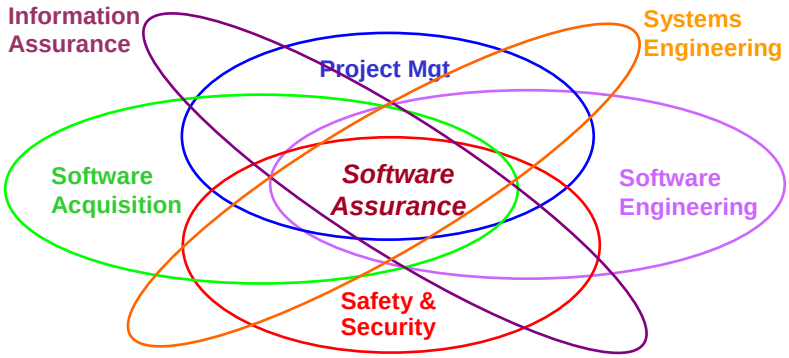
Software Assurance: People

- Provide Software Assurance Common Body of Knowledge (CBK) framework to identify workforce needs for competencies, leverage "best practices," and guide curriculum development for Software Assurance education and training**
  - Hosted Electronic Develop a Curriculum (EDACUM) Event and CBK Working Groups (April, June and August 2005) to develop CBK that involved participation from academia, industry and Federal Government
  - Partitioned domains for "Acquisition & Supply," "Development," and "Post-Release Sustainment"
  - Distribute CBK v0.9 in October 2005 and v1.0 by December 2005
  - Develop CBK awareness materials, including Frequently Asked Questions by January, 2006
  - Develop a pilot software assurance training/education curriculum consistent with CBK in conjunction with early adopters for distribution to Centers of Academic Excellence in Information Assurance Education by September 2007

Homeland Security

**NCSD Goal Action 2.3.1

Disciplines Contributing to SwA CBK



In Education and Training, Software Assurance could be addressed as:

- A "knowledge area" extension within each of the contributing disciplines;
- A stand-alone CBK drawing upon contributing disciplines;
- A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.

Homeland Security

11

Software Assurance: Process

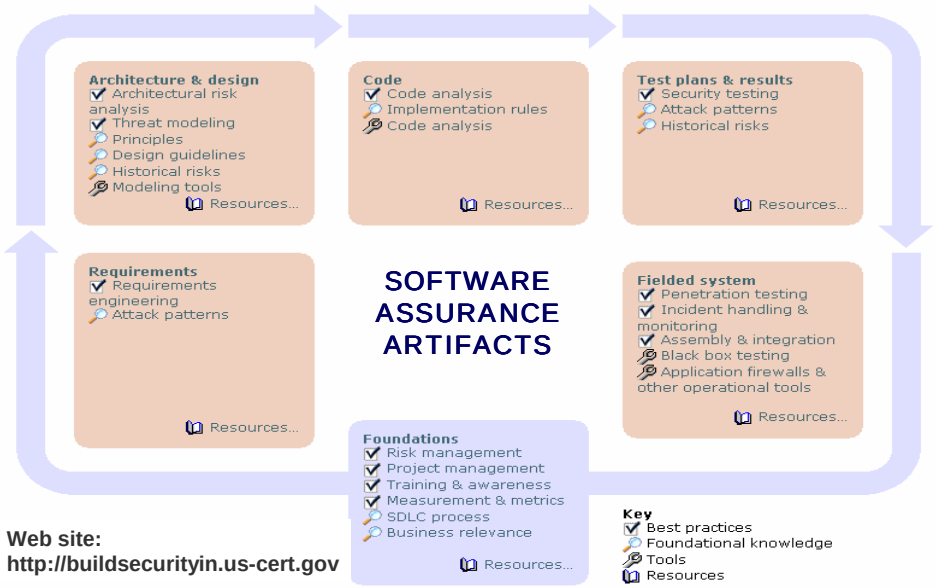
- Provide practical guidance in software assurance process improvement methodologies**
  - Co-sponsor semi-annual Software Assurance Forum for government, academia, and industry to facilitate the ongoing collaboration (April 2005, 3-4 October 2005 and 16-17 March 2006)
  - Collect, develop, and publish practical guidance and reference materials for Security through the Software Development Life Cycle for training software developers in software assurance process improvement methodologies.
  - Sponsoring work with *Software Engineering Institute* and industry to develop a web-based central repository for dissemination of recommended standards, practices, and technologies for secure software development to launch October 2005

**NCSD Goal Action 2.3.2

Homeland Security

12

SwA Process: Lifecycle Touch Points



Web site:
http://buildsecurityin.us-cert.gov

Software Assurance: Process (cont.)

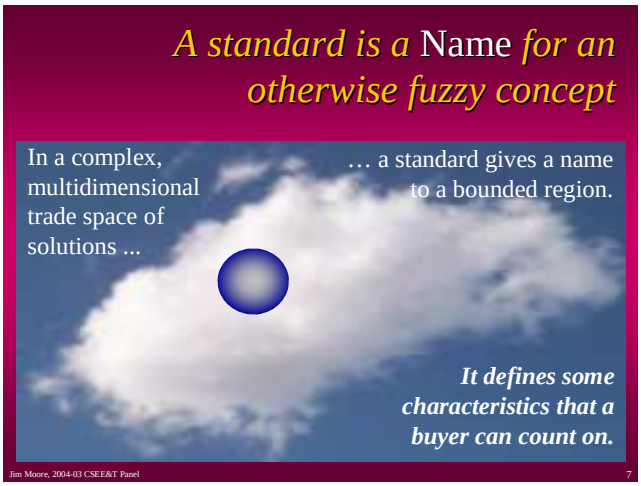
- Provide practical guidance in software assurance process improvement methodologies**
  - Develop a business case analysis to support lifecycle use of security best practices
  - Complete the DHS/DoD co-sponsored comprehensive review of the NIAP (National Information Assurance Partnership) to be published Sep 2005
  - Participate in relevant standards bodies; identify software assurance gaps in applicable standards from IEEE, ISO, NIST, OMG, CNSS, and Open Group and support effort through DHS-sponsored Processes and Practices Working group (April, June, August, October, and December 2005 and March, June and September 2006)

Homeland Security

**NCSD Goal Action 2.3.2

14

Value of Standards



- ***Software Assurance*** **needs standards to assign names to practices or collections of practices.**
- **This enables communication between:**
  - **Buyer and seller**
  - **Government and industry**
  - **Insurer and insured**

Homeland Security

Standards represent the "minimum level of responsible practice," not necessarily the best available methods

15

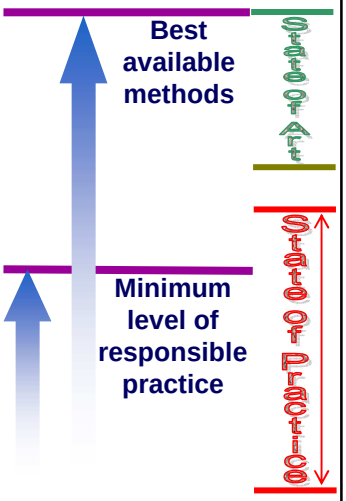
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

Raising the Ceiling

- *Information Assurance, Cyber Security* and *System Safety* typically treat the concerns of the most critical system assets.
  - They prescribe extra practices (and possibly, extra effort) in developing, sustaining and operating such systems.

Raising the Floor

- However, *some* of the concerns of *Software Assurance* involve simple things that any user or developer should do.
  - They don't increase lifecycle costs.
  - In many cases, they just specify "stop making avoidable mistakes."



*[1] Adopted from Software Assurance briefing on "ISO Harmonization of Standardized Software and System Life Cycle Processes," by Jim Moore, MITRE, June 2, 2005, *[2] US 2nd National Software Summit, April 29, 2005 Report (see http://www.cnsoftware.org) identified major gaps in requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art and gaps in state-of-the-art and state-of-the-practice

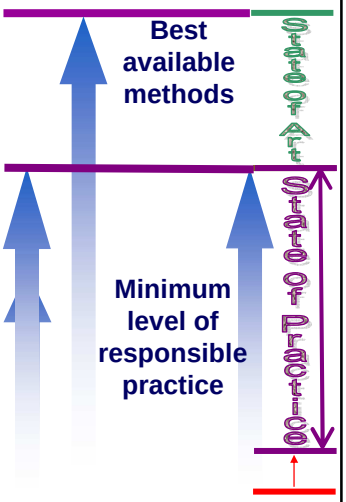
Using Standards and Best Practices to Close gaps between state-of-the-practice and state-of-the-art *1, 2

Raising the Ceiling

- *Information Assurance, Cyber Security* and *System Safety* typically treat the concerns of the most critical system assets.
  - They prescribe extra practices (and possibly, extra effort) in developing, sustaining and operating such systems.

Raising the Floor

- However, *some* of the concerns of *Software Assurance* involve simple things that any user or developer should do.
  - They don't increase lifecycle costs.
  - In many cases, they just specify "stop making avoidable mistakes."



*[1] Adopted from Software Assurance briefing on "ISO Harmonization of Standardized Software and System Life Cycle Processes," by Jim Moore, MITRE, June 2, 2005, *[2] US 2nd National Software Summit, April 29, 2005 Report (see http://www.cnsoftware.org) identified major gaps in requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art and gaps in state-of-the-art and state-of-the-practice

New Scope of ISO/IEC 15026

- New Terms of Reference for the revision of ISO/IEC 15026, "System and Software Assurance:

System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.

Adopted from Paul Croll's SSTC 2005 presentation, "Best Practices for Delivering Safe, Secure, and Dependable Mission Capabilities"

Homeland Security

18

Safety/Security Meta-Practices for ISO/IEC 15026*

1. Ensure Safety and Security Competency
2. Establish Qualified Work Environment
3. Ensure Integrity of Safety and Security Information
4. Monitor Operations and Report Incidents
5. Ensure Business Continuity
6. Identify Safety and Security Risks
7. Analyze and Prioritize Risks
8. Determine, Implement, and Monitor Risk Mitigation Plan
9. Determine Regulatory Requirements, Laws, and Standards
10. Develop and Deploy Safe and Secure Products and Services
11. Objectively Evaluate Products
12. Establish Safety and Security Assurance Arguments
13. Establish Independent Safety and Security Reporting
14. Establish a Safety and Security Plan
15. Select and Manage Suppliers, Products, and Services
16. Monitor and Control Activities and Products

* Represents a synthesis/harmonization of 4 Security Standards with 4 Safety Standards

Safety and Security Extension to Integrated CMMs: adapting standards-based practices

- *Common Criteria for Information Technology Security Evaluation,* Part 3: Security assurance requirements, Version 2.1, Common Criteria Project Sponsoring Organizations, 1999.
- *Defence Standard 00-56, Safety Management Requirements for Defence Systems,* Ministry of Defence, United Kingdom, December 1996.
- *IEC 61508, Functional Safety of electrical/electronic/programmable electronic safety-related systems,* International Electrotechnical Commission, 1997.
- *ISO/IEC 17799:2000(E): Information technology – Code of practice for information security management,* International Organization for Standardization, First edition 2000-12-01.
- *Military Standard System Safety Program Requirements,* MIL-STD-882C, United States Department of Defense, January 1993.
- *Risk Management Guide for Information Technology Systems,* National Institute of Standards and Technology, Special Publication 800-30, 2001.
- *Standard Practice for System Safety*, MIL-STD-882D, United States Department of Defense, February 2000.
- *Systems Security Engineering Capability Maturity Model®, SSE-CMM®*, Model Description Document, Version 3.0, June 15, 2003. *(ISO/IEC 21827)*

Safety and Security Goals & application practices

Goal 1. An infrastructure for safety and security is established and maintained.

AP 1 Ensure safety and security awareness, guidance and competency.

AP 2 Establish and maintain a qualified work environment that meets safety and security needs.

AP 3 Establish and maintain storage, protection and access and distribution control to ensure the integrity of safety and security information.

AP 4 Monitor operations and environmental changes, report and analyze safety and security incidents and anomalies, and initiate corrective actions.

AP 5 Establish and maintain plans to ensure continuity of business processes and protection of assets.

Goal 2. Safety and security risks are identified and managed.

AP 6 Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.

AP 7 For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.

AP 8 Determine, implement, and monitor the risk mitigation plan to achieve an acceptable level of risk.

Safety and Security Goals & application practices

Goal 3. Safety and security requirements are satisfied.

AP 9 Determine applicable regulatory requirements, laws, standards, and policies and define levels of safety and security.

AP 10 Develop and deploy products and services that meet safety and security needs, and operate and dispose of them safely and securely.

AP 11 Objectively verify and validate the work products and delivered products and services to assure safety and security requirements have been achieved and services fulfill intended use.

AP 12 Establish and maintain safety and security assurance arguments and supporting evidence throughout the life cycle.

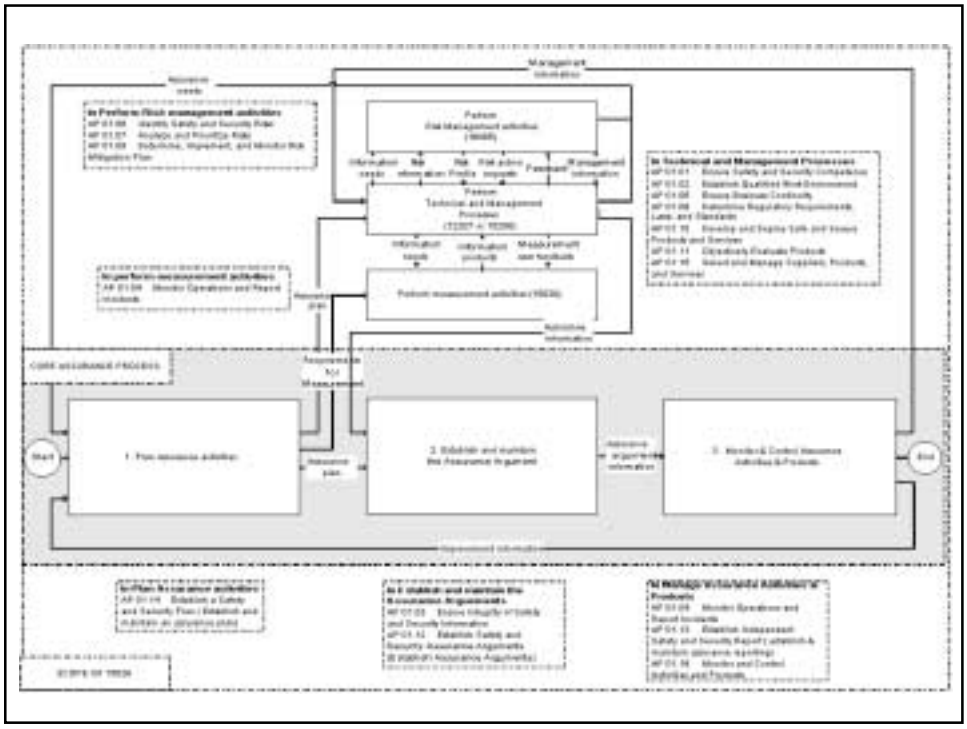
Goal 4. Activities and products are managed to achieve safety and security requirements and objectives.

AP 13 Establish and maintain independent reporting of safety and security status and issues.

AP 14 Establish and maintain a plan to achieve safety and security requirements and objectives.

AP 15 Select and manage products and suppliers using safety and security criteria.

AP 16 Measure, monitor, and review safety and security activities against plans, control products, take corrective action, and improve processes.



Assurance Process Require Security Measurement

- Systems and products that have not been evaluated within a security context need to have safety re-evaluated
- Technical and Management Processes (12207/15288) must contribute to the assurance argument and need measurement support
- The treatment of vulnerabilities and threats (Safety Hazards and Security Threats) is handled as Risk Management (16085)
- Measurement activities need more explicit support for security
  - beyond ISO 15939
  - Information Security Measurement is needed to support Assurance activities

Homeland Security

Why Measure Security?

"Whatever approaches are used to improve cyber security, measuring their success would appear to be essential to determining how effective they are and to making improvements.

However, fundamental problems exist with measuring success in security….." *

[* CRS Report for Congress on 'Creating a National Framework for Cybersecurity: An Analysis of Issues and Options' Feb 22, 2005]

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Information Needs – First Level

Are the residual security risks assigned to a defined entity acceptably low, for defined security threats?

What is the Return on Security Investment (ROSI) ?

relates the achieved integrated security performance of an entity (systems plus processes) with the total security costs incurred (development and operations)

At the next level of decomposition, we can ask the following questions:

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Information Needs – Second Level

1. What is the capability/competence of the resources deployed on security?
2. Are security actions based on known best practice and in compliance with applicable standards and legal requirements?
3. How are security risks being managed?
4. What is the assurance evidence that defines our degree of confidence in likely future security performance?
5. What is the achieved performance of our systems in terms of managing threats, vulnerabilities, responding to events and recovering from & controlling damage?

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Objectives of PSM Security Measurement

1. Review current status of work of TWG
2. Review security and how it might be measured
3. Sketch measurement approach proposed
4. Next Steps

Current Status of TWG Effort

- Security TWG met in Feb 2004 and July 2004
- Draft White Paper v1.0 issued on 30th November 04. To be discussed tomorrow, then update to v2.0
- White Paper reviews types of security measurement and strategy for developing measures; 'scoping and shaping' exercise
- Work still to be done in collaboration with security specialists: review strategy; develop measurement constructs; indicators mapped to artifacts etc.; measurement information specs.

What is Security? *

- Computer security: protection of the systems and data stored therein against unauthorized access, modification, destruction or use [Turn 1986]
- A 'secure' information system is one where the risks of specific undesired outcomes to its assets have been reduced to an acceptable level [Chivers 2004]
- Security is multi-faceted
  - Privacy, Anonymity
  - Multi-level security
  - Authentication
  - Integrity
  - Availability
  - Audit, Accountability

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Security of What?

- Information/ software intensive systems
- Stand alone PC
- Local networks, single organization
- Information systems
- Large networks, supply chains
- Internet, www, e-business, cyberspace
- Embedded systems
- Control systems
- Critical infrastructure
- Government, military systems

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Current Trends

- Stand-alone or isolated systems -> distributed, networked information systems, web-based services, cyberspace
- Grid, pervasive/ ubiquitous, mobile, software agents
- Hierarchical control - > collaboration, e-business, processes that cut through organizational structures
- Critical systems & services increasingly dependent on cyberspace
- Increasing complexity – systems not fully understood
- Post 9/11, Enron - > increased risk perception

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Implications for Security - 1

- Increasingly difficult to define and police ‘boundaries’
- Digital world is abstract – more difficult to authenticate, requires trust in supporting systems, services
- Attackers exploit all aspects of systems (especially human weaknesses), not only the digital
- Security a property of total systems (including organizations, communications, people), not only the computers
- Vulnerabilities associated with the interfaces, links, shared services, complexity
- Increasing overlap of safety and security in many sectors
- Historical development of the internet, sw/ hw technology has not prioritized security

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Implications for Security - 2

- Security is vulnerable to small, local failures: ‘weakest link’ property
- The damage resulting from a security incident can be distant in time and space; and difficult to assess
- Security is improved by use of particular technologies, components, protocols, systems. But no technology is completely secure. Therefore need ‘security processes’
- Attackers are learning agents – dynamic aspect; ‘battle of learning curves’; attackers can be geographically remote
- Concerned with system operations, as well as with system development projects
- Attackers can exploit automation and share information rapidly

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

How is security achieved?

Depends on the attack threat and the defended assets

Types of defense:

- Improve quality of implementations, particularly software
- System design modifications to mitigate security risks
- Security functions implemented in security-specific components
- Tamper-resistant hardware
- Modifications to organizational processes, security-specific processes
- Societal processes (legal system, risk/economic system, cultural aspects)

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Example Technologies

- Encryption (algorithms, keys)
- Protocols (e.g. to set up encrypted connections)
- Computer security; access control, multi-level security models, security kernels
- Identification & Authentication (passwords, biometrics, tokens)
- Defenses against network-sourced attacks on computers: malware, viruses, worms, trojan horses, malicious mobile code (e.g. patches, firewalls, intrusion detection)
- Web security – cookies, web scripts
- Internet security - IP security, DNS encryption, e-mail security
- Public key infrastructure

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Methods used in Security Engineering

- Threat modelling (threat trees)
- Vulnerability scanning
- Risk assessment to prioritize
- Security policy/ strategy
- Lifecycle analysis
- Trust models
- Develop countermeasures; protection, detection & response
- Implement countermeasures
- Test, V&V, independent V&V
- Assess performance and improve/ adapt

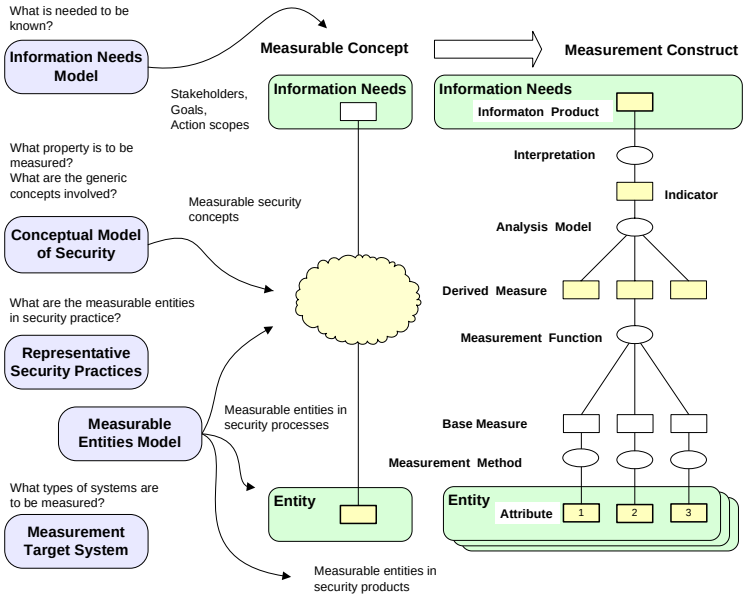
* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Why PSM?

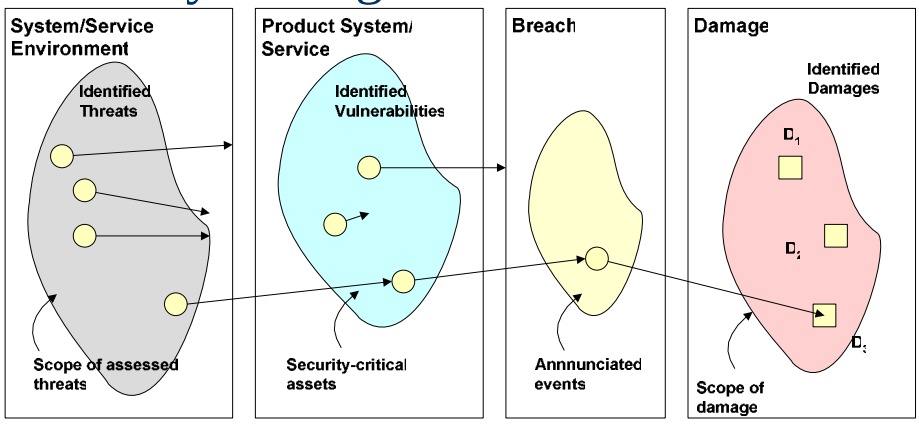
- Measurement experience based on practice
- Provides communication between technical/ engineering specialties and management (project, process, enterprise, acquisition)
- Process-based, with a feedback loop
- Provides a platform for integration between specialties, and with systems engineering; between different sub-specialties within security engineering
- Explicit measurement constructs, therefore can be changed
- Compatible with compartmentalization

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

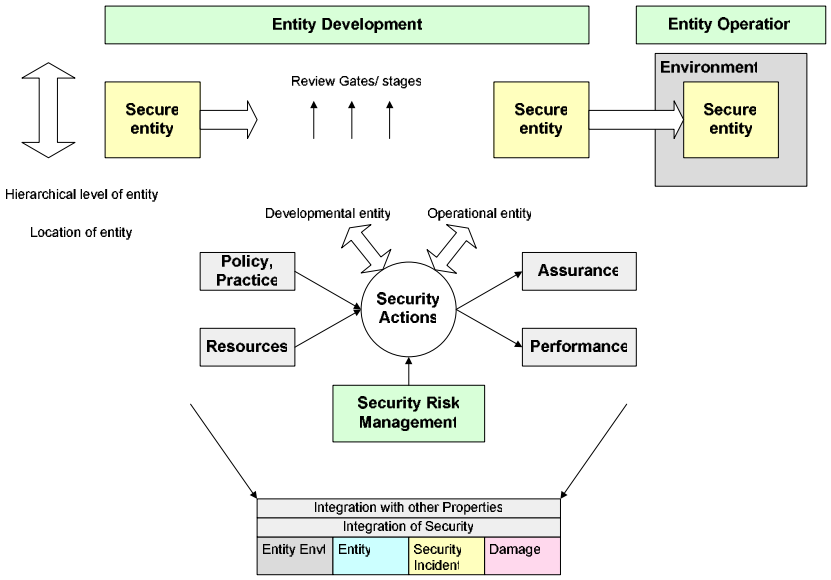
Security Measurement Constructs



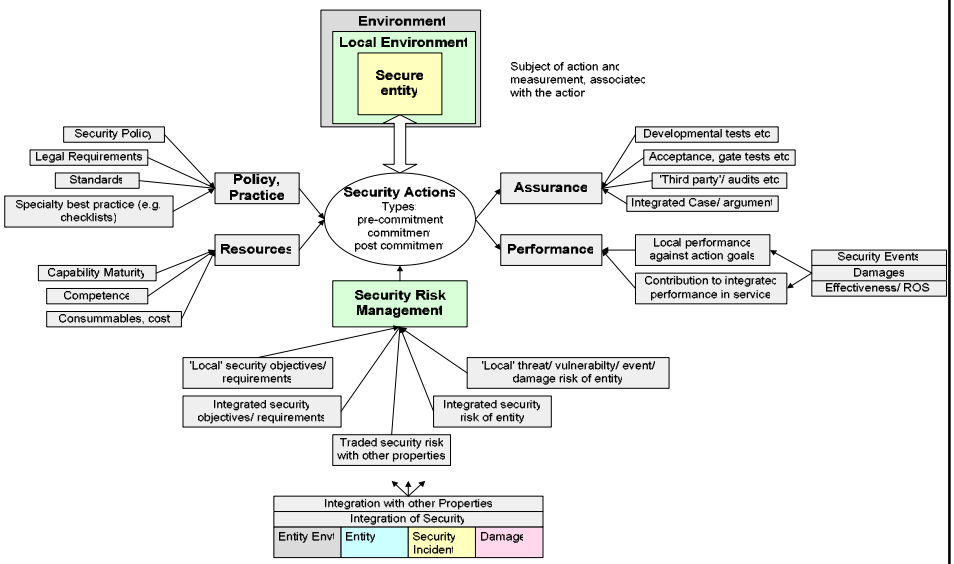
Security Managed Domains



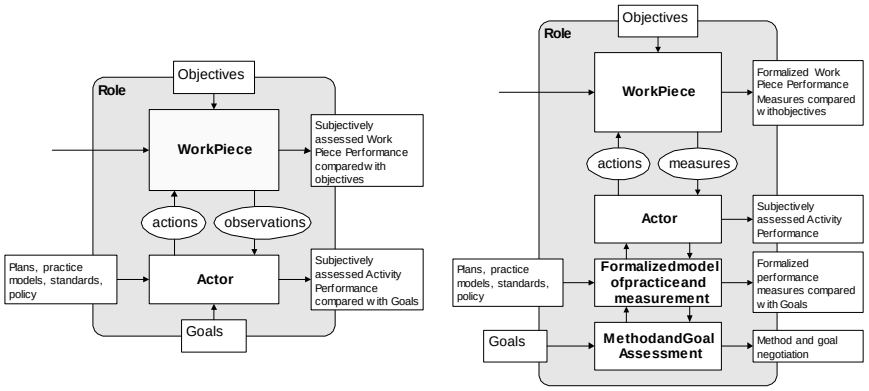
Types of Security Measurement



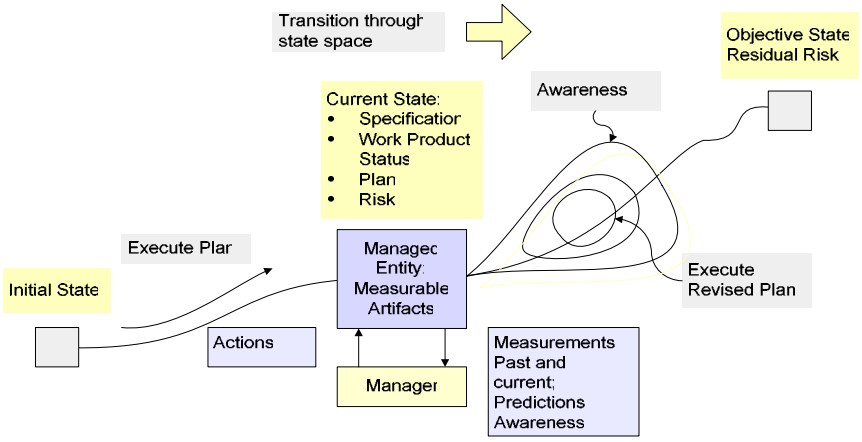
Development of Measurement Framework



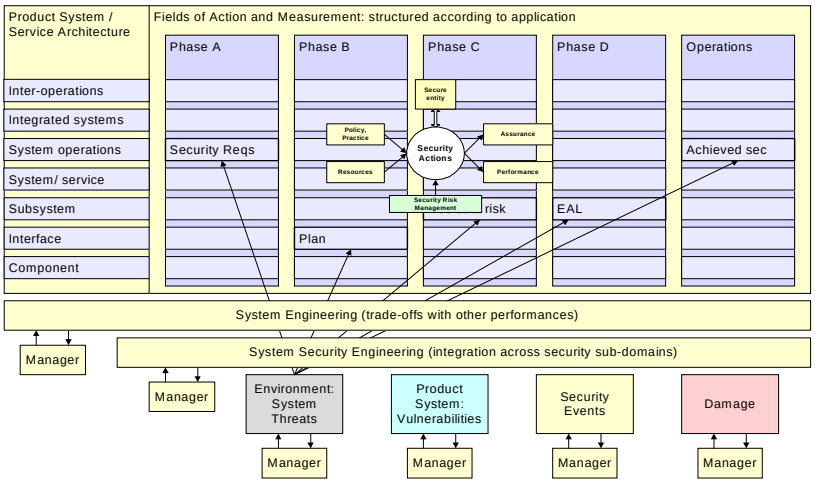
Measurement Development



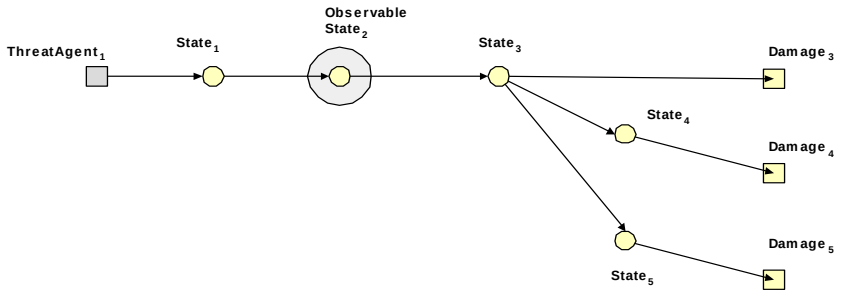
Project



Security Measurement & Complex Projects



Measurement against Attack Scenarios



ISO/IEC JTC1/SC27 **N4474**

REPLACES: N4188

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	Text for Working Draft
TITLE:	**Text for ISO/IEC 2nd WD 27004* — Information technology — Security techniques — Information security metrics and measurements**
SOURCE:	Project Editors (Eva Kuiper, Paloma Llaneza)
DATE:	2005-06-30
PROJECT:	27004*
STATUS:	In accordance with resolution 3 (contained in SC 27 N4599) of the 17th SC 27 Plenary meeting in Vienna, 2005-04-18/19, this document is being circulated for **STUDY AND COMMENT**. The national bodies and liaison organizations of SC 27 are requested to send their comments/contributions on this Working Draft directly to the SC 27 Secretariat by **2005-10-07.**

Next INCITS Metrics Team Conference Call is Aug 2, 1 pm Eastern

ISO/IEC TC JTC1/SC 27 N **4474**

Date: 2005-05-20

ISO/IEC WD 27004.2

ISO/IEC TC JTC1/SC 27/WG 1

Secretariat: ANSI

Information technology — Security techniques — Information security management metrics and measurements

1 Introduction

Information Security is a process and so should be managed. Adopting an Information Security Management Systems (ISMS) should be a strategic decision for any organization. This standard intends to facilitate the management of an ISMS by providing a method for defining implementation objectives and effectiveness criteria, tracking and measuring its evolution over time.

This International standard specifies *measurements* and measurement techniques that may be used by an organization to facilitate the management of ISMS by providing measurement process model that uses objective information to monitor and review the performance and effectiveness of the ISMS, processes and controls. This document provides guidance on how an organization, through the use of metrics, may identify the adequacy of in-place security controls, policies, and procedures and develop a program to measure Information Security performance. Its goal is to explain the metric development and implementation process and so assist in the creation of a metric program that can assist management when making decisions about the effectiveness and efficiency of security controls. The use of this standard will allow organizations to answer the question how effective and efficient the organization's ISMS is and what degree of implementation and maturity has been achieved. Use of measurements will allow comparison of achieved information security outcomes over a period of time and between similar business areas in the organization as part of continuous improvement. The use of Information Security Management Metrics and Measurements (IS3M) is an ongoing process of collection and assessment of data and information to provide a current evaluation of performance, as well as performance trends over time. In contrast, ISMS audits are conducted periodically to verify conformance to defined requirements.

ISO/IEC TC JTC1/SC 27 N **4474**

Date: 2005-05-20

ISO/IEC WD 27004.2

ISO/IEC TC JTC1/SC 27/WG 1

Secretariat: ANSI

Information technology — Security techniques — Information security management metrics and measurements

Additionally, ISMM may provide input into information security risk management processes, prioritisation of security investment and changes to security implementation. Such changes may be necessary to:

1. reduce the probability or impact of security incidents;
2. reduce vulnerability to particular threats or
3. improve the lower costs of existing controls and management processes.

This International Standard supports the requirements of ISO ISMS Specifications, especially in the Check phase of the PDCA cycle. Information Security Management Measurement (ISM measurements) and ISMS audits supports the management of an organization to assess the status of its information security performance and to identify areas of improvement. While this standard should be highly relevant and useful to organisations implementing ISMS according to the Standard ISO/IEC 27001, its applicability should not be limited to this. The standard should be applicable to any organisation that has an information security management programme and that wishes to make measurements concerning information security management.

2 Scope

This standard specifies metrics and provides guidance concerning measurement procedures and techniques applicable to determining and describing the effectiveness of information security controls, information security processes, and information security management systems. It is intended to be applicable to any organization that has a need to take actions to protect the security of information. It is intended to be used in conjunction with standards specifying requirements for: information security management systems, information security process reference models, and management of information.

Information Security metrics are based on performance goals and objectives. Information Security performance goals state the desired results of an information security program implementation. Information Security performance objectives enable accomplishment of goals by identifying practices defined by security policies and procedures that direct consistent implementation of security controls across the organization. Information Security metrics monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities and identifying possible improvement actions.

The objective of this document is to provide guidance on how an organization, through the use of metrics, measurements, and appropriate measurement techniques, can assess its security management status. It is intended to produce repeatable, comparable and reasonable results. It explains the integration into the information security management system (ISMS), the metric process, and – most important – provides guidelines on how one can determine a business object's security status.

NOTE 1. Whenever in this Standard the terms "ISMM", "ISM measurement" or "measurements" is used, the whole range of metrics, indicators and measures is meant [i.e. base measures, derived measures, metrics and indicators] unless a specific type of document is referred to.

NOTE 2. Throughout this Standard the abbreviation IS3M is used to cover the "Information security management metrics and measurements" term.

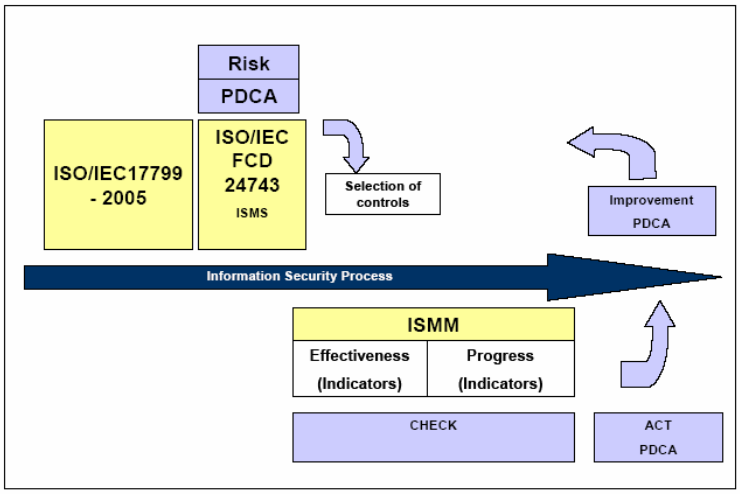


Figure 1 How ISMM fits into the information security process within an organization in conjunction with ISO/IEC17799 and ISMS according to the PDCA cycle and risk assessment

ISO/IEC TC JTC1/SC 27 N 4474
Date: 2005-05-20
ISO/IEC WD 27004.2
ISO/IEC TC JTC1/SC 27/WG 1
Secretariat: ANSI
Information technology — Security techniques — Information security management metrics and measurements

2.2 Objective

The objectives of the process are:

- Control (the effectiveness and the lower costs of existing controls of the process and procedures, of implementation and operate with the security management policy) by means of measures and the report of information.
- Analyse and understand (security management status, degree of effectiveness and the lower costs of security controls, provide evidence for security management audits; provide work visibility and results in the field of security).
- Predict (the time and cost of a project, the increase in resources, anticipate needs, prioritise actions for improvement or security initiatives)
- Improve (security in information).

2.3 Application

This Standard is applicable to different management styles and organizational environments. It has been organised in such a way that its contents may be adapted to the requirements of any organization and any specific management style.

The requirements set out in this International Standard are generic and are intended to be applicable to all organizations with ISMS, regardless of type, size and nature of business.

ISO/IEC TC JTC1/SC 27 N 4474
Date: 2005-05-20
ISO/IEC WD 27004.2
ISO/IEC TC JTC1/SC 27/WG 1
Secretariat: ANSI

Information technology — Security techniques — Information security management metrics and measurements

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- ISO/IEC 17799:2005, Information technology – Security Techniques - Code of Practice for Information Security Management
- ISO/IEC 27001:200?, Information technology - Security techniques - Information security management systems requirements

4 Terms and definitions

For the purposes of this Guide, the terms and definitions given in ISO/IEC 15939:2002, ISO/IEC 27001:2005, ISO/IEC 14598-1:1999, ISO/IEC 17799:2005 and the following apply.[1]

Challenges for Security Metrics

- Count the number of successful attacks, but ‘critical’ attacks may be comparatively uncommon, so that absence of a successful attack may not indicate effective security
- attackers often take steps to avoid detection, so an absence of detected attacks may in fact be a measure of poor rather than good security
- alternatives: proxy measures, such as how well technology, policy, and activities conform to certain accepted benchmarks
- proficiency testing, such as blind "red team" attacks or other penetration testing
- difficult to identify appropriate metrics; also risks of distortions that may be associated with any particular metric

[CRS Report - adapted]

Some Insights about Measurement

- Organizations can be really good at implementation measures; yet not effective at outcome performance & really not good at linkages
- Senior leadership needs to spend enough time identifying what is important to mission success and needs to communicate it effectively to providers
  - Need to identify what is important to them
  - Need repeatable ways to communicate & track
  - Need dedicated investment in management of the process
- Bottom up→quantitative, standards driven, tool based implementation of collection mechanisms
- Top down→qualitative, simplified, yet tied to ‘real data’
- Need to have a good understanding of risk & a good way to frame investment decisions in terms of risk to mission, function, resources
- Measurement can seem to be really complicated; especially when not enough time is spent on analysis

Elements of a Measurement Strategy

- Adopt PSM as an integrating framework, measurement process
- Develop a structured measurement framework for security, building on existing frameworks (NIST, S&S extensions to CMMI, ISO standards)
- Develop reference base measures in collaboration with security specialist communities
- Develop reference target system model to define scope, boundaries
- Adopt a control-theoretic model – learning loop that includes management action and measurement; engage with identification of information needs; msmt models derived in real-time
- Three-level model – measurement against plan, risk management, consequence/uncertainty management
- Performance measurement wrt attack scenarios (near misses)

* Based on Security Measurement Progress Report presented to the PSM TWG, by John Murdoch, The University of York, 23 March 2005

Program Leadership Responsibilities

"Operate today, plan for tomorrow,
invest for the future & guide the transformation"

-Minimize Risk to Mission-

Requires:

1. **Understanding of the operational environment *(operations)***
   - **What should I invest in <u>now</u> to mitigate risk to operations?**
2. **Knowledge of gaps between as-is and to-be *(strategy)***
   - **What investments do I need to make for <u>tomorrow</u>?**
3. **Assumed Risk (today vs. tomorrow) *(risk mitigation)***
   - **What are the residual risks *(risk exposure)* to be accepted?**
   - **What are the tradeoffs in terms of <u>risk to mission</u>?**

Today's Vulnerabilities

-systemic vulnerabilities -

Perimeter Security

- Policy (ports & protocols)
- Technology (IDS, firewalls…)
- Patch Management
- Configuration Management
- Password Management

Remote Access

- Wireless Services
- VPN connections
- dial-up access
- dual-use laptops

Protecting Critical Servers

- Domain Controllers
- Legacy applications
- Integrated UNIX/Windows domain authentication

Data Management

- "hard & crunchy on the outside, soft & gooey on the inside"

Social Engineering

Core Principles for a Successful Executive-Level Measurement Program

- Measures of progress must be tied to goals that are important to management.
- Staff should understand the importance of the goals and the role of the measurement in accomplishing them (help them to become excited).
- Executive-level metrics should be understandable to management.
- Metrics are indicators that the goals are being achieved - they are not themselves the goals.
- It's important to find good metrics - bad metrics can impede progress towards the goals (outcome & goal focused)
- Metrics will likely change as progress is made towards the goals.
- Tracking metrics requires gathering and analyzing data periodically (quarterly) - establish efficient mechanisms to do this.
- Different parts of organizations will require varying levels of detail - try to establish executive level metrics that are rollups or extracts from lower level metrics. Lower level organizations should own the metrics at their level.

Next Steps for Security Measurement

1. Review & improve framework in PSM White Paper on Security Measurement
   - ❑ White Paper offered as a starting point for discussion; framework, strategy for developing security measures
   - ❑ Expressions of need for (and caution about) security metrics
2. Plan how to develop measures in different security areas; prioritization; collaboration
3. Participate in development of NIST and ISO Security Measurement standards
4. Develop example measurement specifications based on particular security practices/ standards, and particular technologies (e.g. software development, CC security functional components)
5. Develop PSM paper(s) on Measuring Software Security Attributes and Enterprise Security Measurement
6. Test measurement proposals and improve by means of project trials
7. Develop integrated practical guidance on how to develop security measures; scenarios to illustrate the provision of indicators to meet management needs in making decisions regarding security
8. Update PSM documents to reflect explicit inclusion of security measurement

Software Assurance: Technology

- Enhance software security measurement and assess Software Assurance testing and diagnostic tools**
  - Collaborate with National Institute of Standards and Technology (NIST) to inventory software assurance tools and measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts
    - – Host workshops with NIST to assess, measure, and validate the effectiveness of tools
  - Develop R&D requirements for DHS S&T consideration; coordinating Software Assurance R&D requirements with other federal agencies
    - – Fund a R&D project (through the DHS S&T Directorate) that will examine tools and techniques for analyzing software to detect security vulnerabilities.
    - – Include techniques that require access to source code, as well as binary-only techniques
  - Collaborate with other agencies and allied organizations to mature measurement in security

**NCSD Goal Action 2.3.3

Homeland Security

62

Software Assurance: Acquisition

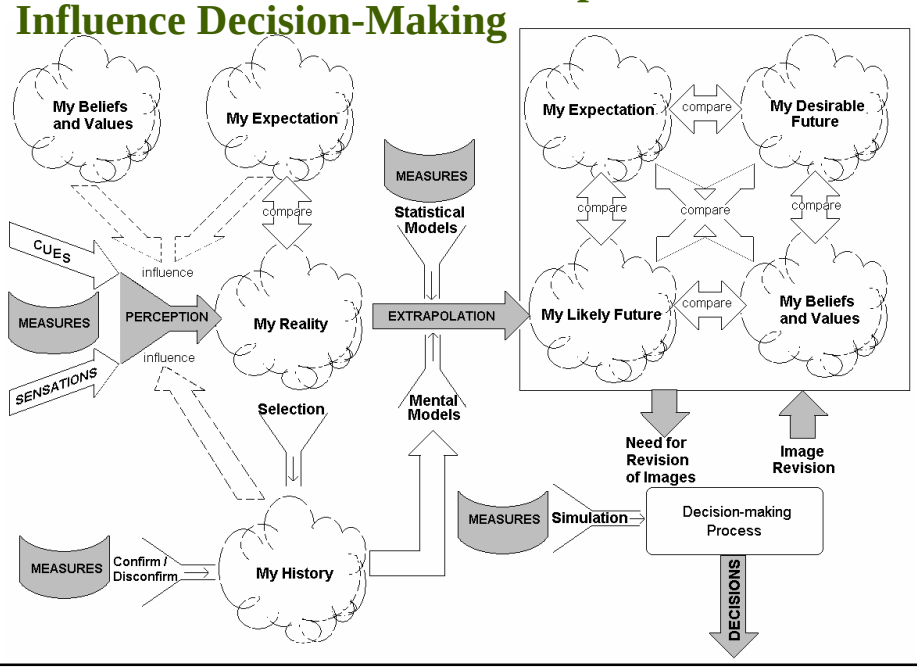
- Enhance software supply chain management through improved risk mitigation and contracting for secure software**
  - Develop and disseminate templates for acquisition language and evaluation based on successful models
  - Develop and disseminate common or sample statement of work / procurement language that includes provisions on liability for federal acquisition managers
  - Provide materials to organizations providing acquisition training and education

Homeland Security

**NCSD Goal Action 2.3.4

63

Measurement Influences Perceptions that Influence Decision-Making



Security Measurement

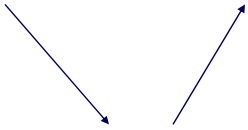
- Systems security is an intricate part of today's business infrastructure
- Systems security performance is needed to support business operations
- The ability to measure and then manage that performance is essential
- Security measurement is required for assurance processes needed for system & software engineering, risk mgt and program mgt
- Developing security practices that address the System/Software Development Life Cycle (SDLC) and the organization's IA and cyber security objectives creates an opportunity to leverage existing efforts and realize significant capability improvements
- Providing supporting measurement for Cyber Security and IA Capability Management will support decision-making and provide return on investment

Guess What?…

SOFTWARE VULNERABILITIES OUTPACE CAPABILITIES TO REMEDY THEM: Microsoft issued 40 security patches for IE and 13 security patches for Outlook during the course of 15 months AND In 15 months there were 261 listed vulnerabilities for Microsoft O/S. 92 were vulnerable to user action; 169 vulnerable to network award code exploits

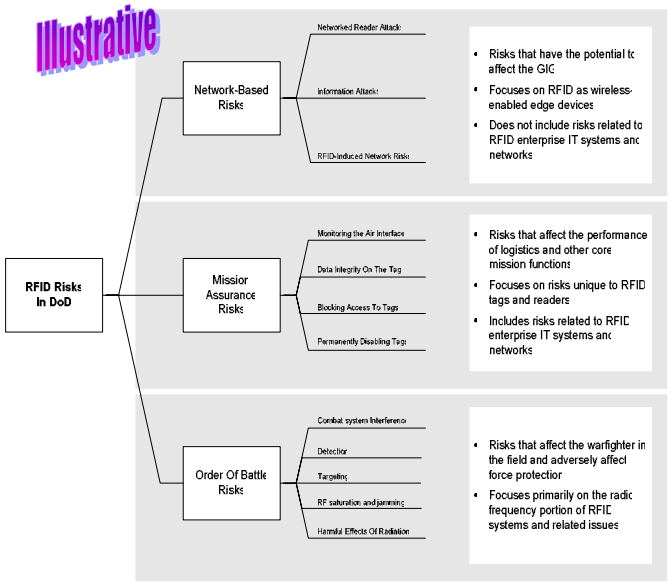
CURRENT IAVM PROCESS IS NOT EFFECTIVE: Patches existed for 12 of 14 worms analyzed in that exploited network aware code.

Cost – Risk - Benefit



Real Problem

RFID Security Taxonomy: Three Areas Of Concern



- Network-Based Risks are related to traditional network security risks already being addressed by the IA community
- Mission assurance risks become important as the department becomes increasingly dependent on AIT

Reaching the Stakeholders

Leverage Efforts in Evolving ISO Standards, CNSS IA and IEEE CS SWEBOK

Education	Professional Development	Training and Practices
• Curriculum • Accreditation Criteria	• Continuing Education • Certification	• Standards of Practice • Training programs
CNSS IA Courseware Evaluation	***CSDP Online Prep Course***	***IEEE Software and Systems Engineering Standards Committee***
IEEE/ACM Software Engineering 2004 curriculum	***IEEE CS SWE Book Series***	***ISO/IEC JTC1/SC7 & SC27 and other committees***
ABET	***Certified Software Development Professional***	
University acceptance	**Individual acceptance**	**Industrial acceptance**

Adopted from "Integrating Software Engineering Standards" material prepared by IEEE Computer Society Liaison to ISO/IEC JTC 1/SC 7, James.W.Moore@ieee.org, 23 February 2005

Software Assurance Observations

- Business/operational needs are shifting to now include "resiliency"
  - Investments in process/product improvement and evaluation must include security
  - Incentives for trustworthy software need to be considered with other business objectives
- Pivotal momentum gathering in recognition of (and commitment to) process improvement in acquisition, management and engineering
  - Synergy of good ideas and resources will continue to be key ingredient
  - Security requirements need to be addressed along with other functions
- From a national/homeland security perspective, acquisition and development "best practices" must contribute to safety and security
  - More focus on "supply chain" management is needed to reduce risks
    - National & international standards need to evolve to "raise the floor" in defining the "minimal level of responsible practice" for software assurance
    - Qualification of software products and suppliers' capabilities are some of the important risk mitigation activities of acquiring and using organizations
  - In collaboration with industry, Federal agencies need to focus on software assurance as a means of better enabling operational resiliency

Homeland Security

71

Government Perspective of Software Assurance

- Significant government/industry interest in Software Assurance
- Continue to leverage all sources of software, but reduce risk
  - Raise level of trust for all software
  - Minimize vulnerabilities and understand threat
- DHS and DoD in conjunction with other federal agencies are identifying and specifying SW Assurance processes/practices and SW-enabled technologies to mitigate risks

- Software Assurance common body of knowledge needed to support education and training, and lifecycle management
- Continue to collaborate with industry, academic institutions and international allies

Homeland Security

72

Homeland Security

www.us-cert.gov

Joe Jarzombek, PMP
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126

Software Assurance Web site:
http://buildsecurityin.us-cert.gov

Software Assurance Research & Development

- Groupings
  - Development processes
  - Scanning/detection of vulnerabilities
  - Countermeasures
  - Development tools
  - Application Environment
  - Requirement/Design/Validation
  - Education and Training
  - Secure Kernel

Homeland Security

Software Assurance Research Agenda – High Assurance

- Develop more cost-effective methods for high assurance software development.
- Compose secure systems from independent secure components.
- Improve binary scanning tools.
- Truly trustworthy computing base.
- Develop methods to minimize/control the functionality of product.

Homeland Security

Software Assurance Research Agenda –

- Develop cost effective methods for improving software development (improved binary scanning tools, source scanning, correct by construction)
- Compose secure systems from independent secure components (trustworthy computing base)
- Minimize/control functionality
- Detect/counter run-time vulnerabilities
- Practical processes and measurement for software dependability and defensibility (safety, security, and survivability).
  - Has assurance improved?
  - Which approach is better and by how much?
  - How assured is the organization, program, or system?
  - Time to exploit?

Homeland Security

76

Software Assurance Research Agenda – Product Diagnostic Capabilities

- Process must have:
  - Meaningful results (trusted)
  - Criteria
  - Multiple Options for assurance levels
- Software Evaluation
  - Assumes a prioritized list of critical assets
  - Important to look at all critical software
  - Need lifetime evaluation/monitoring of software
  - Need to influence R&D
  - Resource constrained

Homeland Security

77

Software Assurance Research Agenda – Secure Kernels

- Establish levels of assurance
- Work to eliminate “where applicable” clauses, and enforce current guidance.
- Enable vendor/consortium investment augmented by federal funding to achieve highly assured and certified products.
- New paradigms are needed for evaluation.
- Different kinds of secure kernels are needed:
- Investigate if the secure infrastructure components (such as the Kernel, PCS, CORBA, DDS, Web Services, etc.) need to be part of the Net Ready KPP.

Homeland Security

78

IT R&D (ITRD)
National Coordination Office (NCO)

- Sponsored by the Office of Science and Technology Policy (OSTP)
- Tasked with coordination of IT research across Federal Government
- Current members
  - **NITRD Agencies:**
    - **NSF, NASA, NSA, NIH, DARPA, and NIST**
  - **Non-NITRD Agencies:**
    - **FAA, FDA, AFRL, ARO and ONR**
- More Information
  - www.itrd.gov

NSF – National Science Foundation
NASA – National Aeronautics and Space Administration
NSA – National Security Agency
NIH – National Institute of Health
DARPA – Defense Advanced Research Projects Agency
NIST – National Institute of Standards and Technology
FAA – Federal Aviation Administration
FDA – Food and Drug Administration
AFRL – Air Force Research Lab
ARO – Army Research Organization
ONR – Office of Naval Research

High Confidence Systems and Software (HCSS)

- One of several ITRD Interagency Working Groups, HCSS focus:
  - Affordable and predictable high levels of safety, security, reliability, and survivability
  - Applicable to critical domains such as aviation, healthcare, national defense, and infrastructure.
  - POC: Dr. Helen Gill, hgill@nsf.gov
- Coordinating Activities
  - NA/CSTB study on Sufficient Evidence? Building Certifiably Dependable Systems A two-part HCSS activity focused on medical devices
  - Possible Aviation Safety Workshop
  - Tentative Workshop on Supervisory Control Systems

HCSS Coordinating Activities

- Software Verification Grand Challenge:
  - Make verification a basic technology for achieving a high degree of assurance for large-scale software
  - Workshop held Feb 2005, Working Conference planned for Oct 2005
- Supervisory Control Systems
  - Planning session Oct 05
  - Workshop January-March 2006

HCSS Multi-agency Activities

- Jointly Funded
  - DARPA, NIST, and NSF are supporting a new NAS/CSTB Cyber Security study
  - NSF and DARPA are co-funding two Cyber Trust projects:
    - Methods for showing that large software systems are free from certain security flaws
      - Stanford University, U. of Maryland, and UC Berkeley
    - SecureCore project investigates trustworthy operation of mobile computing devices, spanning a range of security requirements and design constraints:
      - Pocket devices, Secure embedded systems, and mobile computing devices
      - Integrated design of the processor hardware, the operating system kernel software, and the networking interface.
      - Princeton, Naval Postgraduate School, USC/ISI
  - NSF and DHS are co-funding the DETER/EMIST* network testbed and experimental framework for network security research

*DETER - Defense Technology Experimental Research (DETER) testbed
EMIST - Evaluation Methods for Internet Security Technology (EMIST)

Summary of Individual Agency Activities – National Science Foundation

- Cyber Trust effort
  - Foundations, Network security, Systems software, and Information systems.
- Science of Design
  - Design of software-intensive computing, information, and communications systems.
- Disciplinary research in:
  - Distributed Computing, Embedded and Hybrid Systems,
  - Networking
  - Foundations of Computing Processes and Artifacts
- New FY 2006 Plans include:
  - Basic and technology research for high-confidence embedded systems, hybrid control, distributed systems

Summary of Individual Agency Activities – National Security Agency

- NSA Information Assurance Research Group (IARG) promotes HCSS research activities
  - Trusted Development
  - Containment
  - Hosted the 5th Annual HCSS Conference
- FY 2005 plans also include:
  - Continued joint sponsorship of the National Academies Study on software certification
  - Initiation of joint sponsorship of Open Verification activities with HCSS CG members
  - Sponsored research in Transparency, and High Assurance Platforms

Summary of Individual Agency Activities – National Aeronautics and Space Admin

- Low- to mid-technical readiness level (TRL) programs
  - Computing, Information and Communications Technology Program (CICT)
- Mid-TRL
  - Reusable infrastructure for flight and ground software for the launching of a mission to Mars in 2005.
  - Software Assurance Research Program (Office of Safety and Mission Assurance)
  - Software assurance practices for auto-generated code, COTS integration, and reused or heritage software; reliability of operating systems;
- High-TRL
  - Software Engineering Initiative (SEI) program
  - Software Assurance Technology Center (SATC)

Summary of Individual Agency Activities – Defense Adv Research Proj Agency

- Self-Regenerative Systems (SRS)
  - Intrusion-tolerant systems that gracefully degrade and recover after an attack by reconfiguring and self-optimizing
  - Technical areas include
    - Biologically-inspired diversity;
    - Cognitive immunity and healing systems
- Security Aware Systems
  - System smoothly adapts to changing resources, building blocks, security requirements, mission goals, and threats.

Summary of Individual Agency Activities – National Institute of Standards & Technology

- Software Diagnostics and Conformance Testing Division (SDCTD)
  - Electronic Commerce
  - E-Health includes Health Level Seven (HL-7) standards and conformance and establishment of a standards roadmap
  - National Software Reference Library (NSL)
  - Pervasive Computing
  - Test Method Research
- NIST's Computer Security Division (CSD)
  - Security technologies
  - Systems and Network Security
  - Management and Assistance Program
  - New CSD opportunities include:
    - Standard Reference Model (SRM) for source code security
    - Trust and confidence taxonomy toolkit for reliability, interoperability, security, etc.

Summary of Individual Agency Activities – Federal Aviation Administration

- Under the Office of the Assistant Administrator for Information Services and CIO (AIO)
  - In FY 2004 AIO activities included
    - Developing a rapid quarantine capability
    - Establishing an integrity and confidentiality lab to test wireless information systems security to aid the develop of an agency policy
    - Extending COCOMO II (COnstructive COst MOdel II) to include security
    - Identifying requirements for a biometrics single sign-on
    - Validating web data mining to find FAA vulnerabilities
  - In FY 2005 AIO work will continue FY 2004 activities and include:
    - Implementation of a rapid quarantine capability
    - Testing biometrics single sign-on
    - Testing behavior-based security
    - Developing an Information Systems Security Architecture (ISSA)

Summary of Individual Agency Activities – Food and Drug Administration

- Research areas of interest are:
  - Safety and safety modeling
  - Certification issues
  - Forensic analysis
- Specific research projects include:
  - Proton beam therapy device (safety and modeling)
  - Software for an infusion pump with a control loop which led to an initiative of similar control loop software for a ventilator device (certification)
  - Blood bank software regulation (certification)
  - Reverse engineering of C programs to look for inconsistencies and errors in radiation treatment planning systems used in tumor treatment (forensics)
  - Unintended function checker (with NSA) (forensics)

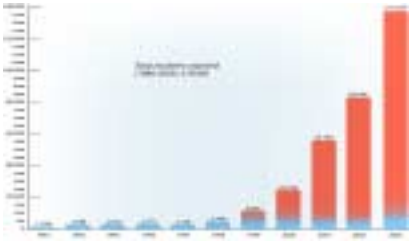
Conclusions on SW Assurance R&D

- Software Assurance is an active interest across the Federal Government
  - Multiple centers of research and transition
  - Advertised research projects
- Ample opportunities exist for software assurance research
  - Fault tolerant architectures
  - Forensics
  - Certification

Homeland Security

Growing Cost of Vulnerabilities

Incident Reports



Vulnerabilities Reports

***Hacker attacks** cost the world economy a whopping **$1.6 trillion in 2000**.*

PricewaterhouseCoopers, 2000

U.S. virus and worm attacks cost **$10.7 billion** in the first three quarters of 2001. The **CodeRed Worm alone has cost $2.6 billion** globally in 2001.

Computer Economics, 2001

In 2003, the CMU CERT CC reported 137,529 attack incidents and 3,770 vulnerabilities

Carnegie Mellon University
Computer Emergency Response Team Coordination Center

*If anything,CERT statistics may understate the problem, because the organization counts all related attacks as a single incident. **A worm or virus like Blaster or SoBig, a self-replicating program that can infect millions of computers, is but one event.***

The New York Times, Sep 29, 2003

91

Risk of Asymmetric Attack & Threats:
Changing concepts for safety and security

Cyber attacks can be conceived and planned without detectable logistical preparation… they can be clandestinely rehearsed, and then mounted in a matter of minutes or even seconds…"

(Source: President's Commission on Critical Infrastructure Protection, Oct 97)

SQL SLAMMER WORM

- **Infected 90% of vulnerable computers world-wide within 10 minutes of release ***
- **Doubled in size every 8.5 seconds**
- **Full scanning rate (55M scans/second)**

(Source: GAO, Statement by Robert F. Dacey, Director, Information Security Issues, 24 Jul 03)

Software vulnerabilities can be exploited to threaten U.S. critical infrastructure and defense interests, placing missions at risk, especially in an era of asymmetric warfare and terrorism.

Homeland Security

"Systems that are not secure should have safety reconsidered."

92

Unintended Consequences of Reuse

Reused software -- challenges for qualification and evaluation

- Most software bugs are a result of small oversights by a programmer, and
- Most large software programs are combinations of newer code and old code, accumulated over time, almost as if in sedimentary layers.
- A programmer working years ago could not have foreseen the additional complexity and the interaction of software programs in the Internet era;
- yet much of that old code lives on, sometimes causing unintended trouble.

Steve Lohr, "To Fix Software Flaws, Microsoft Invites Attack," The New York Times, Sep 29, 2003

Homeland Security Requires Software Assurance

- Software assurance is required to fulfill security missions and protect critical infrastructure
  - National/federal capabilities dependent on software
  - Exploitable vulnerabilities and malicious code place critical capabilities at risk
  - In era of asymmetric warfare/terrorism, opponents can threaten software-enabled capabilities cheaply & safely
- Federal Sector has software assurance responsibilities
  - Software dependency places assurance at core of national security
  - Federal core competencies must be security-focused in acquiring, procuring and using software *

* October 2002, President's Critical Infrastructure Protection Board IT Security Study Group (ITSSG) identified security shortfalls in acquisition processes and recommended security improvements

Driving Needs for Software Assurance

- Growing concern over the ability of an adversary to subvert the software supply chain
  - Federal Government relies on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements
  - Software development offers opportunities to insert malicious code and/or poorly design and build software enabling exploitation
- Growing concern about capabilities of suppliers to build and deliver secure software with requisite levels of integrity
- Current education & training provides too few practitioners with requisite competencies in secure software engineering
- Growing need to raise the floor and raise the ceiling on software capabilities of the nation
- Processes and technologies are required to build trust into software developed and acquired by Federal Government

Homeland Security

95

NCSD goals from National Strategy & HSPD#7*

	*National Strategy to Secure Cyberspace*					*HSPD-7*
	Priority 1: National Cyberspace Security Response System	**Priority 2:** National Cyberspace Threat and Vulnerability Reduction Prog.	**Priority 3:** National Cyberspace Security Awareness and Training Prog.	**Priority 4:** Securing Govt.'s Cyberspace	**Priority 5:** International Cyberspace Security Cooperation	"…maintain an organization to serve as a focal point for the security of cyberspace.."
Goal 1: Prevent, detect, and respond to cyber incidents, and reconstitute rapidly after cyber incidents.	✓			✓	✓	✓
Goal 2: Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.		✓	✓	✓	✓	✓
Goal 3: Promote a comprehensive national awareness program to empower all Americans to secure their own parts of cyberspace.			✓			
Goal 4: Foster adequate training and education programs to support the Nation's cyber security needs.	✓	✓		✓		✓
Goal 5: Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyber space.	✓	✓	✓	✓	✓	✓

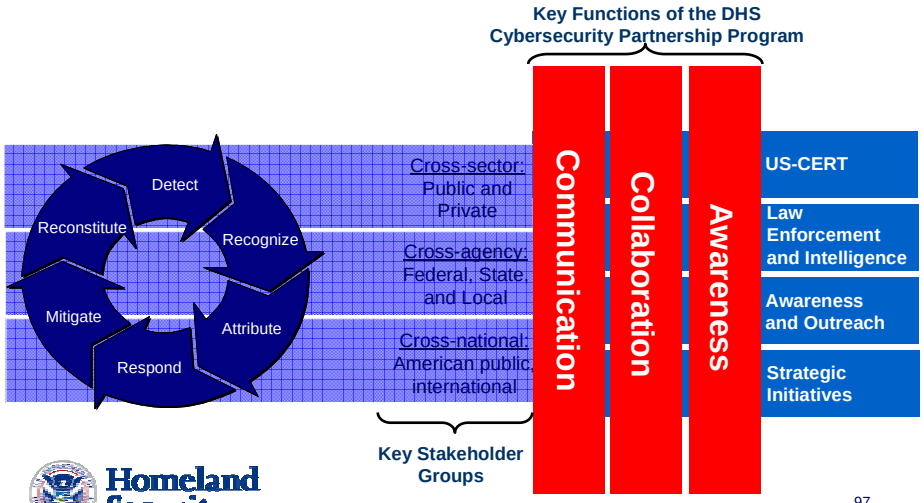
Software Assurance aligned with NCSD goals

Homeland Security

*National Strategy to Secure Cyberspace" and Homeland Security Presidential Directive #7

96

NCSD provides the framework for addressing cyber security challenges & Software Assurance needs



Homeland Security

97

DHS National Cyber Security Division Goal 2:

Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks

- **National Infrastructure Protection Plan** — implementing the cyber component to provide direction to sector specific agencies in developing protection plans and identify critical assets and vulnerabilities in the IT sector
- **Internet Disruption Working Group** — partnership with National Communications System to identify protective measures
- **US-CERT Control Systems Center** — addresses complex security issues associated with the use of control systems present in most critical cyber systems in the nation's infrastructure
- **Control Systems Security and Test Center** — provides a proactive environment for government and industry to collaborate in vulnerability enumeration and reduction activities
- **Software Assurance — developing components (best practices and methodologies, evaluation tools, industry forums) to assist in coordination efforts within the software assurance community**

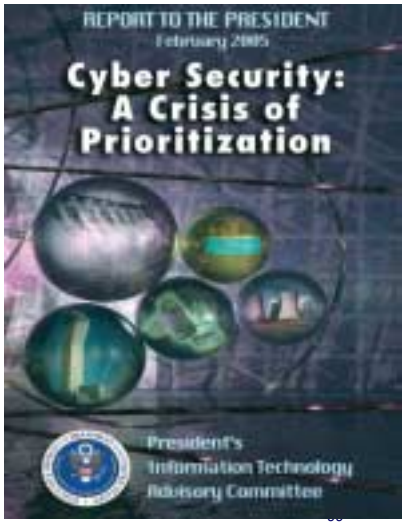
Homeland Security

98

President's Information Technology Advisory Committee Subcommittee on Cyber Security

Areas in Need of Increased Support

- Computer Authentication Methodologies
- Securing Fundamental Protocols
- ***Secure Software Engineering & Software Assurance***
- Holistic System Security
- Monitoring and Detection
- Mitigation and Recovery Methodologies
- Cyber Forensics and Technology to Enable Prosecution of Criminals
- Modeling and Testbeds for New Technologies
- Metrics, Benchmarks, and Best Practices
- Societal, Policy, and Governance Issues



Homeland Security

PITAC* Findings Relative to Needs for Secure Software Engineering & Software Assurance

- Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost.
- Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds of attack programs to compromise millions of computers every year.
- In the future, the Nation may face even more challenging problems as adversaries – both foreign and domestic – become increasingly sophisticated in their ability to insert malicious code into critical software.

*President's Information Technology Advisory Committee (PITAC) Report to the President, "Cyber Security: A Crisis of Prioritization," February 2005

Homeland Security

What has Caused Software Assurance Problem

- Then
  - Domestic dominated market
  - Stand alone systems
  - Software small and simple
  - Software small part of functionality
  - Custom and closed development processes (cleared personnel)
  - Adversaries known, few, and technologically less sophisticated
- Now
  - Global market
  - Globally network environment
  - Software large and complex
  - Software is the core of system functionality
  - COTS/GOTS/Custom in open development processes with reuse (un-cleared, foreign sourced)
  - Adversaries numerous and sophisticated

Homeland Security

101

2nd U.S. National Software Summit
May 10-12, 2004

- Identified major gaps in:
  - Requirements for software tools and technologies to routinely develop error-free software and the state-of-the-art
  - State-of-the-art and state-of-the-practice
- Recommended elevating software to national policy
  - through implementation of “Software 2015: a National Software Strategy to Ensure US Security and Competitiveness”
  - to be pursued through public-private partnerships involving government, industry and academia
  - Purpose of National Software Strategy:
    - Achieve the ability to routinely develop and deploy trustworthy software products
    - Ensure the continued competitiveness of the US software industry

Homeland Security

102

DHS Software Assurance Initiative

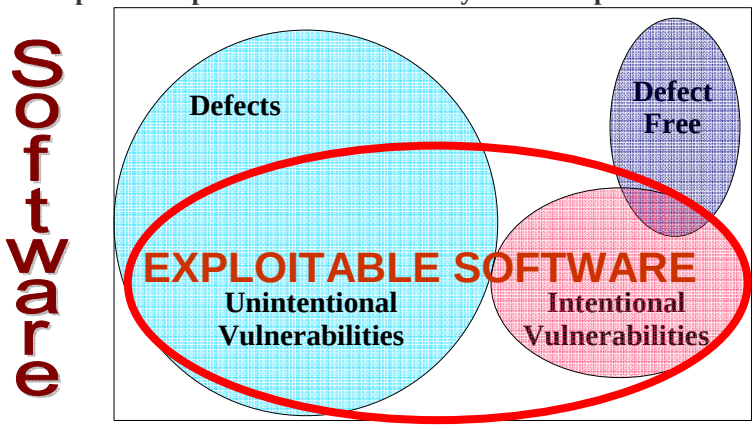
- **Purpose**:
  - Shift security paradigm from Patch Management to Software Assurance
  - Encourage the software developers (public and private industry) to raise the bar on software quality and security
  - Facilitate discussion, develop practical guidance, review tools, and promote R&D investment
- **The National Strategy to Secure Cyberspace - Action/Recommendation 2-14:**

  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."

Homeland Security

Exploitable Software: Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability often independent of "intent"

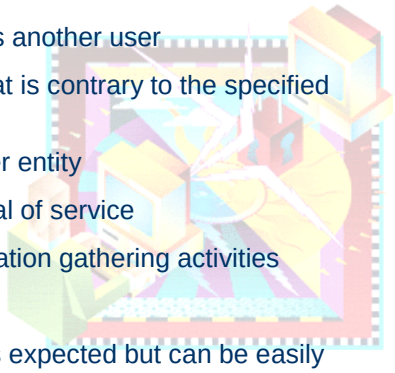


Note: Chart is not to scale – notional representation -- for discussions

Homeland Security

104

Software Vulnerabilities Allow:



- An attacker to execute commands as another user
- Allows an attacker to access data that is contrary to the specified access restrictions for that data
- Allows an attacker to pose as another entity
- Allows an attacker to conduct a denial of service
- Allows an attacker to conduct information gathering activities
- Allows an attacker to hide activities
- Includes a capability that behaves as expected but can be easily compromised
- Is a primary point of entry that an attacker may attempt to use to gain access to the system or data

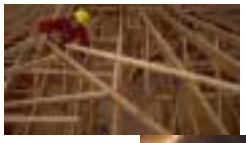
Homeland Security

105

Software Assurance Comes From:

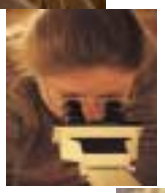
Knowing what it takes to "get" what we want

- Development/acquisition practices/process capabilities
- Criteria for assuring integrity & mitigating risks



Building and/or acquiring what we want

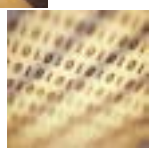
- Threat modeling and analysis
- Requirements engineering
- Failsafe design and defect-free code



Understanding what we built / acquired

- Production assurance evidence
- Comprehensive testing and diagnostics
- Formal methods & static analysis

*Multiple Sources:
OASD(NII)IA,
DHS/NCSD,
JHU/APL



Using what we understand

- Policy/practices for use & acquisition
- Composition of trust
- Hardware support

Homeland Security

106

Software Assurance Lifecycle Considerations

- Define Lifecycle Threats/Hazards, Vulnerabilities & Risks
- Identify Risks attributable to software
- Determine Threats (and Hazards)
- Understand key aspects of Vulnerabilities
- Consider Implications in Lifecycle Phases:
  - Threats to: System, Production process, Using system
  - Vulnerabilities attributable to: Ineptness, Malicious intent, Incorrect or incomplete artifacts, Inflexibility
  - Risks in Current Efforts: Polices & Practices, Constraints

Homeland Security

107