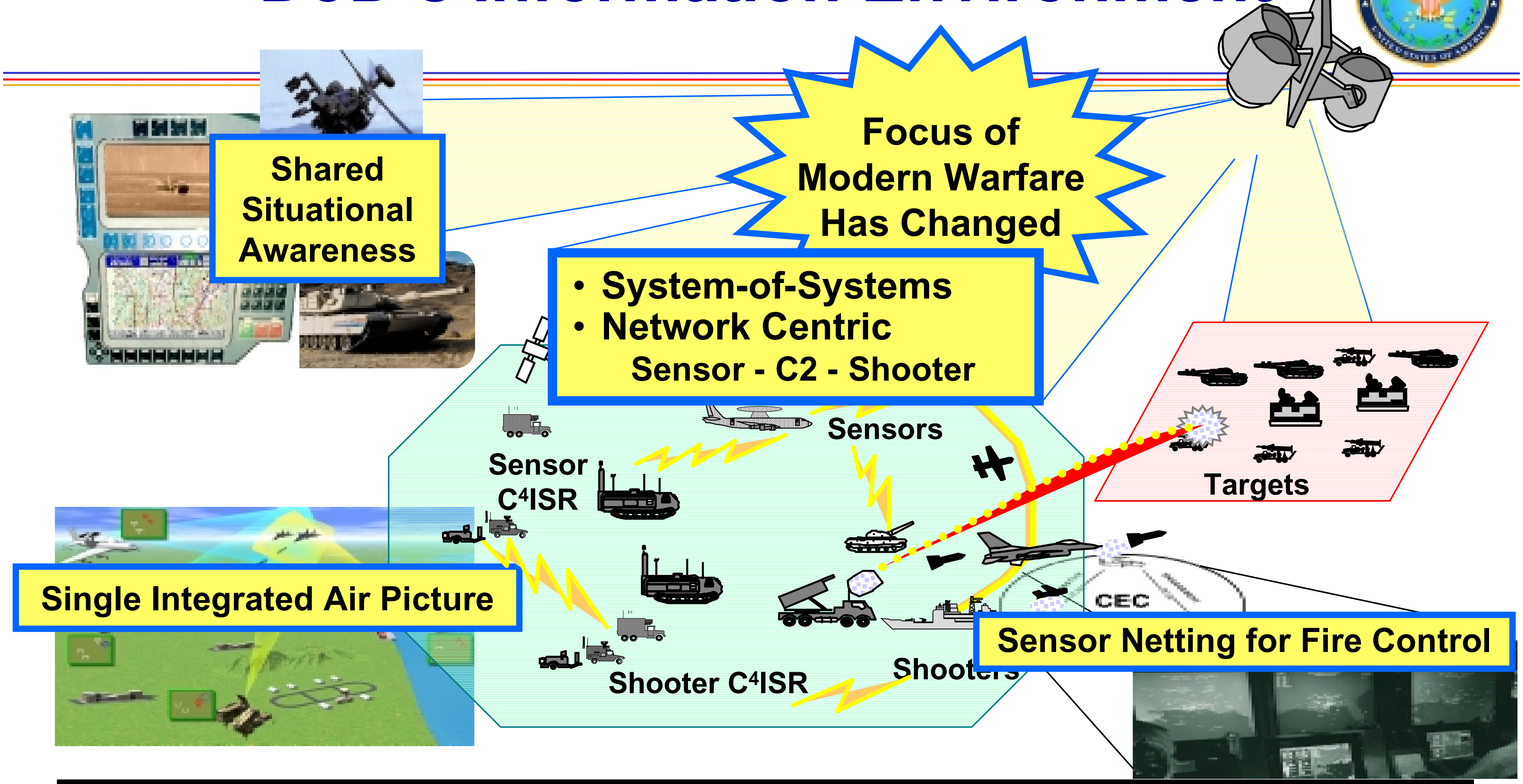
Systems, Networks and Information Integration Context for Software Assurance

Leveraging Collaboration of Initiatives To Ensure Integrity of Systems and Networks

Joe Jarzombek, PMP
Deputy Director for Software Assurance
Information Assurance Directorate
Office of the Assistant Secretary of Defense
(Networks and Information Integration)

Update as of 27 Jan 2004
Managing the Software Assurance Program

DoD’s Information Environment



Focus of Modern Warfare Has Changed

Shared Situational Awareness

- System-of-Systems
- Network Centric
  Sensor - C2 - Shooter

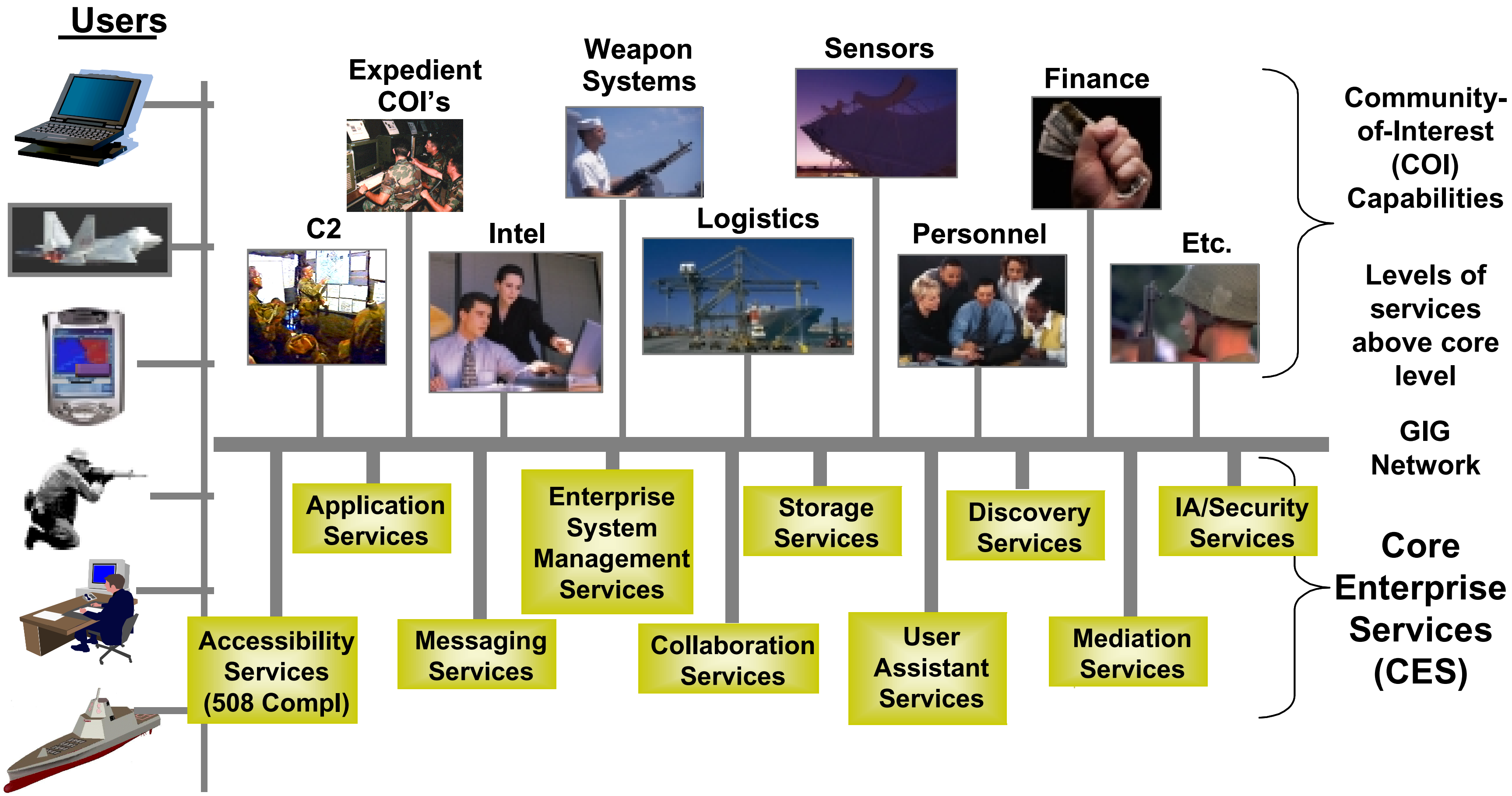
Single Integrated Air Picture

Sensor Netting for Fire Control

- Increasing reliance on IT is increasing vulnerabilities
- GIG: 1 system’s weakness exposes others to danger
- Federal agency info sharing expands vulnerabilities

Net-Centric Enterprise Services

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



Users

Expedient COI's

Weapon Systems

Sensors

Finance

C2

Intel

Logistics

Personnel

Etc.

Community-of-Interest (COI) Capabilities

Levels of services above core level

GIG Network

Application Services

Enterprise System Management Services

Storage Services

Discovery Services

IA/Security Services

Accessibility Services (508 Compl)

Messaging Services

Collaboration Services

User Assistant Services

Mediation Services

Core Enterprise Services (CES)

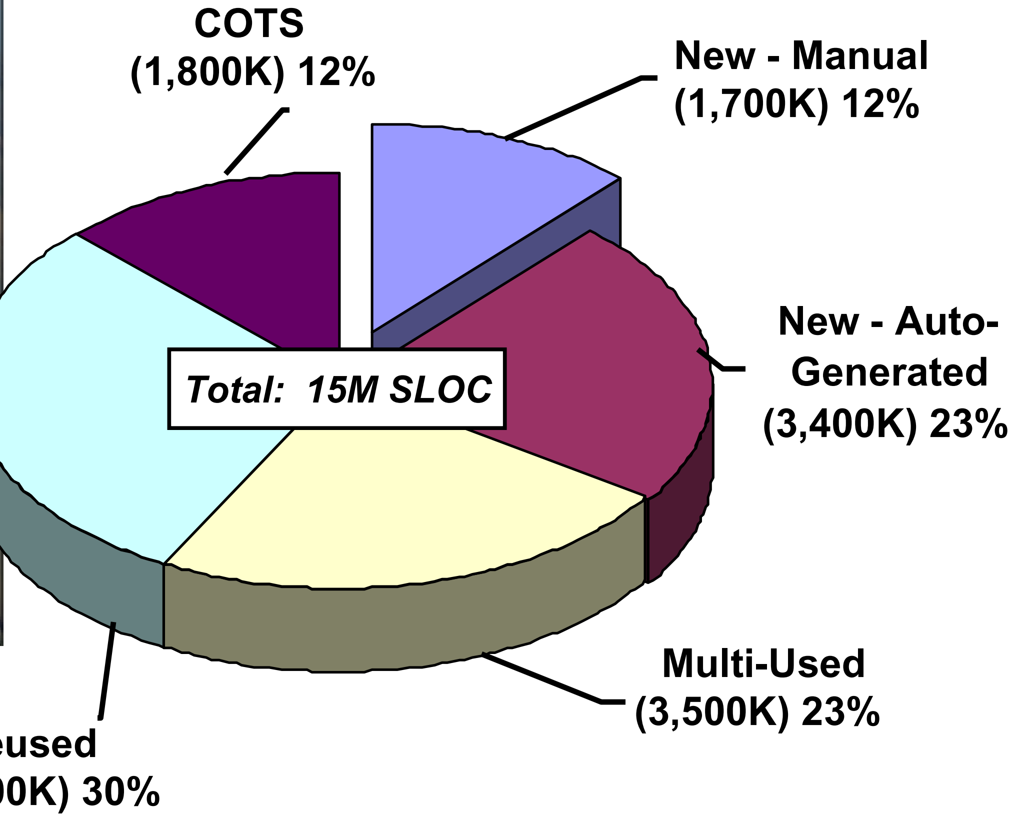
Three Key Trends

- Increasing dependence on COTS software in secure national and DoD information systems
  - Highly distributed (peer-to-peer), net-centric capabilities
  - Increased connectivity multiplies risk
- Increasing code size and complexity
  - No COTS market incentive for time-consuming high assurance production techniques or thorough test
  - Use of current “high assurance” techniques considered inconsistent with acquisition objectives of “faster and cheaper
- Increasing economic incentive for off-shore outsourcing of IT and software development and support

DoD Software Intensive Systems

Employment of Strategy Yields Only 12% Traditional Hand Coding

Joint Strike Fighter
(SLOC by Type)



Software enables capability-based acquisition

Growing reliance on COTS and legacy software reuse

Unintended Consequences of Reuse

- 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

Growing Cost of Vulnerabilities

***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

The CMU CERT Coordination Center reported 76,404 attack incidents in the first half of 2003, approaching the total of 82,094 for all of 2002 in which the incident count was nearly four times the 2000 total.

If anything, the 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

COTS in Secure Systems

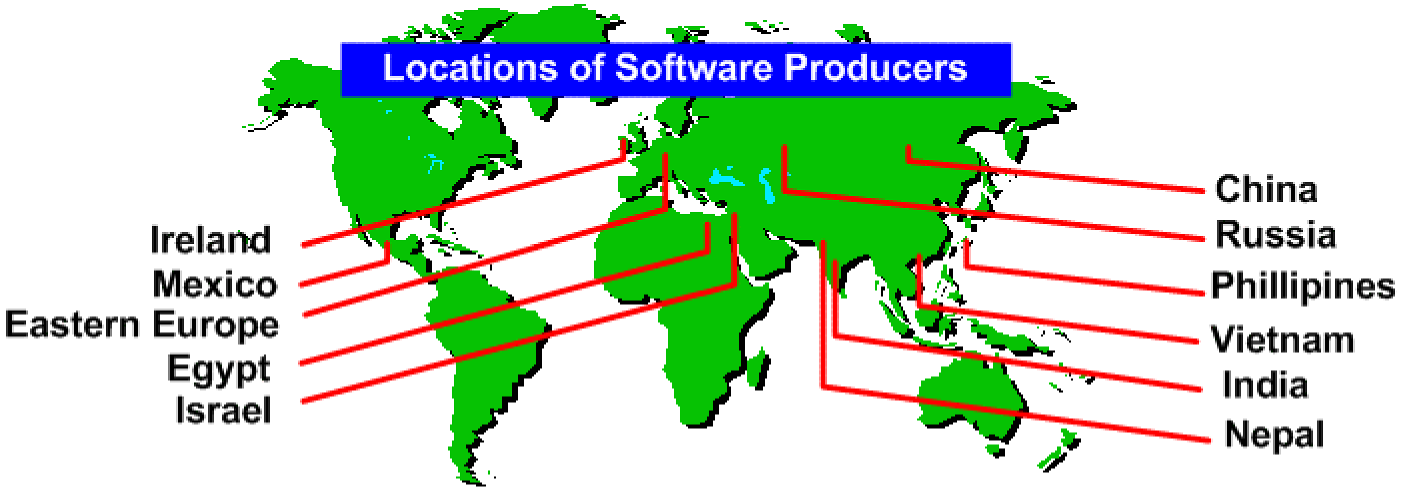
- In the old days - 10 years ago - computer security was mandated
  - Trusted Computing Base / Rainbow Series
  - Outpaced by industry - functionality won over security
- Today, pure COTS solutions are used wherever they are available and applicable
  - COTS security products defend COTS application products
  - Industry is “influenced” to produce more secure solutions
- As functionality becomes available, we lose the ability to operate without it

Increasing Dependence on COTS Software

- DMS: **“… a flexible,** commercial off-the-shelf (COTS)-based application **providing multi-media messaging and directory services..”**
- GCCS: “**… incorporates the latest in**_commercial computer hardware, software, and communications technology**.”**
- NSANet uses ~20 variants of COTS Operating Systems
- NMCI – Microsoft product-based ashore IT infrastructure
  - 70,000 seats at cutover (May 2003); ~400,000 AOR
- SIPRNet and JWICS use TCP/IP Networking
- DISN connectivity provided by CISCO Router OS
- White House voice switching performed by COTS software
- Critical data resides in databases built on COTS software

COTS Off-shore Outsourcing

- Labor is 75% of software development cost
- Equivalent cost of one US SW engineer:
  - Three Indians, four Chinese, or five Russians
- Major producers already use off-shore resources
  - Microsoft, INTEL, IBM, HP, EDS (NMCI contractor)
- Off-shore production predicted to increase 20% annually*



* Computerworld, February 2003

Are Foreign Developers the Only Threat?

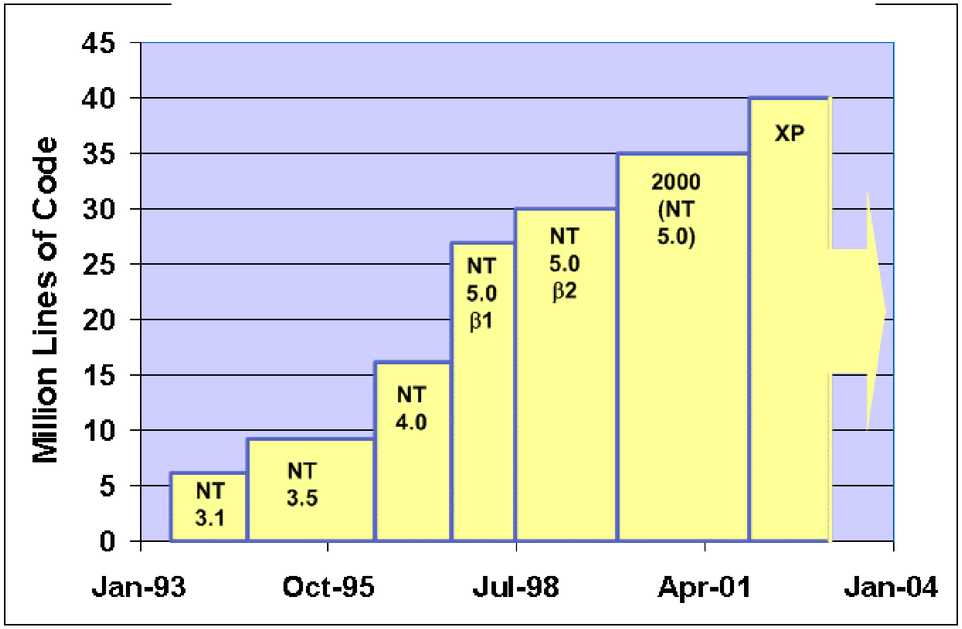
- Approximately 1.2 million software developers in the US*
  - Foreigners and US citizens
- Could we clear them all?
- If they were all cleared, how many would could be “turned”?

* US Department of Labor 2001 Employment Statistics

Code Size and Complexity - Operating Systems

- Microsoft Windows
  - – ~35M LOC
- Solaris 2.6
  - – ~11M LOC
- Linux 2.4*
  - – ~2.5M LOC
- SE Linux
  - – ~2M LOC (Kernel + Security Policy)

Growth in Windows OS Size



* Linux 2.4 has 400 conditional compilation variables, each of which can take on 3 values = 3^{400} possible executable versions.

Code Size and Complexity - Other

- Large non-operating system COTS SW products
  - Network Switch software
  - CISCO Router software
  - Checkpoint Firewall
  - Oracle
  - Internet Explorer
  - Common Compilers
- Is COTS the only threat?
  - STU-III Key Distribution Center
  - Nuclear Explosion Simulations
  - Joint Strike Fighter
  - NSA CES

What About Open Source Software?

- Does access to the source code benefit defenders or attackers more?
  - In a perfect world, reliability growth theory predicts that it will benefit both equally
  - In the real world, there may be asymmetry that benefits the attacker (somewhat)
    - Unpaid beta testers will concentrate on what’s interesting; attackers will concentrate on what’s important to them
- Considering the size of the source code (e.g., 2.4MLOC for Linux 2.4), do open source testers have a chance of fixing all the potential vulnerabilities?
  - Uncoordinated testing

The Tip of the Iceberg

- July 19, 2001: Code Red infects 359,000 Internet hosts in under 10 hours
  - Saturated (found and infected ~all vulnerable hosts)
- January 25, 2003: SQL/Slammer saturates (75,000 Internet hosts) in 10 minutes
  - Speed limited by self-interference
- Slow “contagion” worms could spread as widely without any visible sign
  - Would we know if this had been done?

These examples use only known, “accidental” features of the software. What could be accomplished by design?

Potential Consequences of Malicious Code

- A war predicated on false information inserted in IC databases
- SIPRNet goes down for three days starting on Iraqi Freedom D-day
- More?
  - DoD understands the consequences as well or better than most

Adding Up the Factors

+ COTS provides functionality that we MUST have
+ Little or no insight into COTS software production
  – Foreign influence
+ Most COTS source code unavailable
+ Complexity beyond understanding on practical timescales
  – Results in emergent behavior
  – Obscures purpose (malicious or benign)
  – Precludes exhaustive test

= A critical situation that must be brought under control

Software Assurance Comes From:

Knowing what it takes to build what we want

Development practices and process capabilities

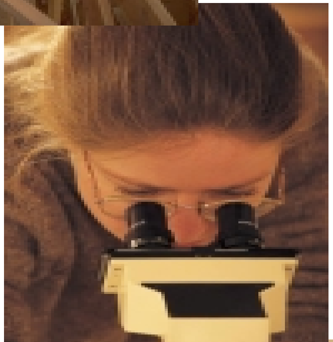
Criteria for assuring integrity

Building what we want

Expressing requirements

Failsafe design

Error-free code

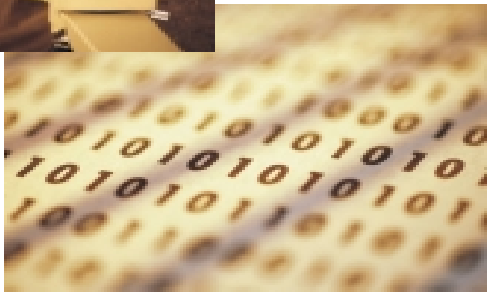


Understanding what we built

Production assurance evidence

Comprehensive testing

Static analysis



Using what we understand

Composition of trust

Trusted path

Hardware support

Policy for use

National Security Requires Software Assurance

- National security depends on computers and networks
  - Many risks to national infrastructure arise from exploitable software vulnerabilities
  - Primary threat is our current lack of technical capability for building and understanding complex software-intensive systems and networks

- Software assurance is required for national security to protect critical infrastructure and secure defense capabilities
  - National security is a federal government responsibility
  - Software assurance is therefore a federal government responsibility; not commercial industry

Need for Software Assurance

- NSA National Computer Security Center has provided a focus for secure software since 1970s
- Many lessons learned in developing software for secure systems were codified in early 1980s in DoD 5200.28 Standard - Trusted Computer Security Evaluation Criteria (the Orange Book)

- -

- National Security Telecommunications and Information Systems Security Policy #11 (NSTISSP-11) uses Common Criteria framework for evaluating COTS products that allow users to trust the broader mass of products.
  - Users write a Protection Profile (PP), a spec of security features
  - Suppliers create a Security Target (security claims)
  - Independent lab evaluates suppliers' claims using increasingly stringent Evaluation Assurance Levels (EALs)

Need for Software Assurance

- Since May 2002, several US federal agencies (DoD, FAA, NASA, DOE), UK MOD, Australian DMO, FFRDCs, & industry have participated in a group co-chaired by DoD & FAA to determine how to provide safety & security assurance extensions to CMMI & iCMM
- In October 2002, the President's Critical Infrastructure Protection Board (PCIPB) created the IT Security Study Group (ITSSG) to review existing acquisition processes, identify significant security shortfalls and recommend a way ahead for security improvements.
- DoD organizations have addressed software assurance issues:
  - to evaluate the ITSSG report and recommend a feasible process that may be integrated into the DoD acquisition process, and
  - to support the GAO review of mitigating risks to software
- In Oct 2003, responsive to DoD & Congressional interests, OASD(NII) established the position for Deputy Director for Software Assurance in the IA Directorate to focus efforts on the Software Assurance Program

DoD's Software Assurance Program
(from Congressional Responses)

"Both foreign and domestic produced software products are vulnerable to having malicious code. Several existing DoD initiatives address these concerns: Software Protection Initiative, Software Producible Initiative, Anti-Tamper Initiative, and the recently established Software Assurance Program:

- DoD in conjunction with DHS will focus on identifying and specifying organizational software assurance processes and software-enabled technologies that are required to ensure systems and network capabilities are secure through a spectrum of threats ranging from vulnerabilities to cyber attacks."
- Software Assurance Program is organized into working groups:
  - WG1 Security Process Capability Evaluation (process focused),
  - WG2 Software Product Evaluation (product focused),
  - WG3 Counter Intelligence (CI) Support
  - WG4 Acquisition/Procurement and Industrial Security, and
  - WG5 User Identification of Protected Assets

Source: US Congressional Hearing on Unconventional Threats and Capabilities, House Armed Services Subcommittee on Terrorism – Bob Lentz OASD(NII) Director for Information Assurance, Sep 22, 2003 response to question from Congressman Martin Meehan (D-MA) on August 8, 2003 "How can we ensure that COTS software is not corrupted by unscrupulous persons or even our allies? How can DoD create secure computing capabilities using COTS software that may have been produced outside the US?

DoD & DHS Interagency Agreement on Software Assurance Program

- Provide analysis of SW assurance problems, the working groups constitute a virtual program team to provide an interagency focus to develop processes to mitigate risks associated with SW vulnerabilities and recommending security improvements.
- Provide requisite interfaces with other software initiatives:
  - DoD Software Protection Initiative
  - DoD Software Producibility Initiative
  - DoD Anti-tamper Initiative
  - government Information Assurance initiatives
  - interagency Safety & Security Assurance process improvement group
  - Government/industry cyber security SW development lifecycle task force
- Work with applicable organizations to coordinate relevant research and intiatives

Software Assurance Program Working Groups -- Leveraging Activities

- **WG1 Security Process Capability Evaluation**
  - Identifying criteria to be used in mitigating risks associated with development capabilities required to deliver secure software
  - Safety & Security Assurance extensions to CMMI & iCMM
    - Practices traceable to 7 source standards
    - Safety & security focus using CMMI & iCMM implementing practices
  - ISO/IEC JTC1/SC7 WG9
    - Redefining its terms of reference to system & software assurance
    - ISO/IEC 15026 to address management of risk and assurance of safety, security, & dependability within context of system and software life cycles
  - NIST Information System Security Project
    - Producing publications on security of Federal Information System
    - Provides standards for labs conducting software product evaluations

* NIST is an agency in the Commerce Department

®Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

Tri-Service Assessment Initiative (TAI) Systemic Analysis -- General Findings

Critical program performance problems

Identified Issues	Relative Occurrence
Process Capability	91 %
Organizational Management	87 %
Requirements Management	87 %
Product Testing	83 %
Program Planning	74 %
Product Quality - Rework	70 %
System Engineering	61 %
Process Compliance	52 %
...	
Configuration Management	26%

Primary causative performance issues are:

Process capability shortfalls - the inability of the program team to design, integrate, and implement processes that adequately support the needs of the program

Need for Extending CMMI® and iCMM® for Safety and Security

- Both CMMI and iCMM provide a framework in which safety and security activities can take place
  - Provide a framework to manage complexity
  - Provide framework for integrated process improvement
  - Provide mechanisms for identifying and managing risks
- Safety and security are critical to both DoD and FAA, as well as other government and industry organizations
- Analysis of current safety and security standards highlighted potential “gaps” in CMMI/iCMM coverage

Need for Extending CMMI® and iCMM® for Safety and Security

- CMMI and iCMM interest in safety/security
  - FAA approved a project to include both safety and security in FAA integrated CMM (iCMM)
  - CMMI Steering Group has discussed addressing safety and security; considerations for future versions of CMMI
- DoD and FAA decided to collaborate on developing safety/security extensions to both iCMM and CMMI
  - Joint FAA/DoD project launched with broad participation including other government agencies, industry, and SEI
  - Objectives: identify best safety and security practices with intent that common content would be included in both models

®Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

Source Documents Selected

- Traceability required between extension and source documents: Demonstrated coverage of source documents
- Three Source Documents for safety
  - *MIL-STD-882C:* System Safety Program Requirements
  - *IEC 61508:* Functional Safety of Electrical/ Electronic/ Programmable Electronic Systems
  - *DEF STAN 00-56:* Safety Management Requirements for Defence Systems
- Four Source Documents for security
  - *ISO 17799:* Information Technology - Code of practice for information security management
  - *ISO 15408:* The Common Criteria (v 2.1) Mapping of Assurance Levels and Families
  - *SSE-CMM:* Systems Security Engineering CMM (v2.0)
  - *NIST 800-30:* Risk Management Guide for Information Technology Systems

Best Practices Synthesized, Harmonized and Reviewed

- Safety and security practices synthesized
  - Source documents for each area mapped together at high-level
  - Practices synthesized from similar practices/clauses/activities pertaining to common outcomes
  - Practice level mappings to source material retained

- Practices harmonized and reviewed
  - Safety and security practices harmonized resulting in common set of practices
  - Distributed for first external review
  - Over 200 comments received from ~35 reviewers in US, Australia, and various European countries
  - Comments dispositioned by team; practices revised
  - Call for Review distributed for second external review

Initial Packaging of Revised Practices

- Revised practices analyzed with respect to reference models
- Most of the harmonized safety and security practices are already addressed to varying extents in existing PAs of CMMI and/or iCMM
  - They can be implemented by performing existing practices of iCMM and/or CMMI, with appropriate interpretation for safety and security assurance application
  - However, there is currently no easy mechanism to identify which practices are required for appraisal or process improvement purposes
- Some practices need more focused coverage in both models
  - Although there is some guidance, additional emphasis is desirable
- Preliminary conclusion:
  - A Safety and Security Assurance Application Area is proposed, and has been drafted
  - A Work Environment Process Area is proposed, and has been drafted

The Safety and Security Assurance Application Area

- Identifies best practices (application practices) associated with the application, drawn from the source documents
  - Provides informative, interpretative information about each application practice
  - Identifies existing practices in one or both reference models that would be performed to implement the application practice
- Keeps the application practices visible for those pursuing the application, for both process improvement and appraisal purposes
- Draws on breadth & depth of reference models for details of required application practices; avoids needless redundancy
- Is appraised by appraising the associated practices in the reference model, as interpreted by the application
  - An application area can be at any capability level

Safety and Security Assurance Application Area

- **Purpose** of Safety and Security (S&S) Assurance
  - establish and maintain a safety and security capability,
  - define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and
  - assure that products and services are safe and secure.

- **Expected AA Outcomes:**
  - Goal 1 – An infrastructure for S&S is established and maintained.
  - Goal 2 – S&S risks are identified and managed.
  - Goal 3 – S&S requirements are satisfied.
  - Goal 4 – Activities and products are managed to achieve S&S requirements and objectives.

NOTE: This is work in progress – see Call for Review package; comments due NLT 1 Mar 2004

Safety and Security Assurance Application Area (cont.)

AA Goal 1 – An infrastructure for S&S is established and maintained.

- AP01.01. Ensure S&S awareness, guidance, & competency.
- AP01.02. Establish and maintain a qualified work environment that meets S&S needs.
- AP01.03. Establish and maintain storage, protection, and access and distribution control to assure the integrity of information.
- AP01.04. Monitor, report and analyze S&S incidents and identify potential corrective actions.
- AP01.05. Plan and provide for continuity of activities with contingencies for threats and hazards to operations and the infrastructure.

AA Goal 2 – S&S risks are identified and managed.

- AP6. Identify risks and sources of risks attributable to vulnerabilities, security threats, and safety hazards.
- AP7. For each risk associated with safety or security, determine the causal factors, estimate the consequence and likelihood of an occurrence, and determine relative priority.
- AP8. For each risk associated with safety or security, determine, implement and monitor the risk mitigation plan to achieve an acceptable level of risk.

Safety and Security Assurance Application Area (cont.)

AA Goal 3 – S&S requirements are satisfied.

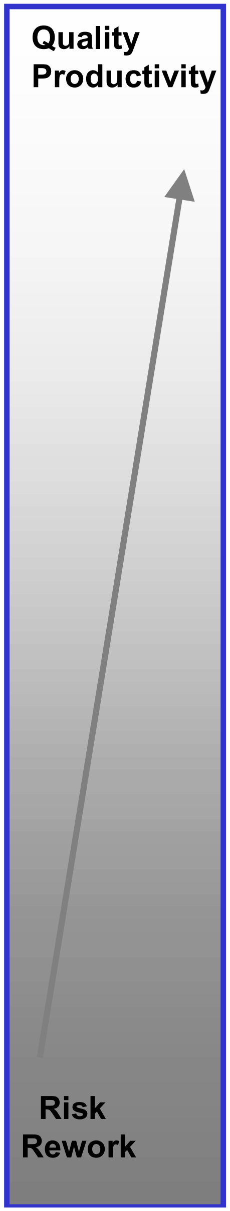
- AP9. Identify and document applicable regulatory requirements, laws, standards, policies, and acceptable levels of safety and security.
- AP10. Establish and maintain S&S requirements, including integrity levels, and design the product or service to meet them.
- AP11. Objectively verify/validate work products and delivered products and services to assure S&S requirements have been achieved & fulfill intended use.
- AP12. Establish and maintain S&S assurance arguments and supporting evidence throughout the lifecycle.

AA Goal 4 – Activities and products are managed to achieve S&S requirements and objectives.

- AP13. Establish and maintain independent reporting of S&S status and issues.
- AP14. Establish and maintain a plan to achieve S&S requirements & objectives.
- AP15. Select and manage products and suppliers using S&S criteria.
- AP16. Measure, monitor and review S&S activities against plans, control products, take corrective action, and improve processes.

CMMI-SE/SW/IPPD/SS Process Areas

Level	Focus	Process Areas
5 Optimizing	*Continuous process improvement*	Causal Analysis and Resolution (CAR) Organizational Innovation & Deployment (OID)
4 Quantitatively Managed	*Quantitative management*	Quantitative Project Management (QPD) Organizational Process Performance (OPP)
3 Defined	*Process standardization*	Organizational Process Focus (OPF) Organizational Process Definition (OPD) Organizational Training (OT) Integrated Project Management (IPM) Risk Management (RSKM) Decision Analysis and Resolution (DAR) Requirements Development (RD) Technical Solution (TS) Product Integration (PI) Product Verification (PV) Validation (VAL) Integrated Teaming (IT) Organizational Environment for Integration (OEI) Integrated Supplier Management (ISM)
2 Managed	*Basic project management*	Requirements Management (REQM) Project Planning (PP) Project Monitoring and Control (PMC) Measurement and Analysis (MA) Process and Product Quality Assurance (PPQA) Configuration Management (CM) Supplier Agreement Management (SAM)
1 Performed		



Safety and Security Assurance: Drawing upon Practices from other PAs

iCMM PAs	CMMI PAs *(including extensions)*
PA 19 Work Environment *(NEW)*	Work Environment *(proposed for CMMI update)*
PA 10 Operation and Support	*Operation and Support (extended from iCMM)*
PA 01 Needs; PA 02 Requirements	Requirements Development *(with new practice to be added)*; Requirements Management
PA 13 Risk Management	Risk Management
PA 08 Evaluation	Verification; Validation
PA 00 Integrated Enterprise Management	*Integrated Enterprise Management (extended from iCMM)*
PA 11 Project Management	Project Planning; Project Monitoring and Control; Integrated Project Management
PA 05 Outsourcing; PA 12 Supplier Agreement Management	Supplier Agreement Management
PA 03 Design	Technical Solution
PA 17 Information Management	*Information Management (extended from iCMM)*
PA 16 Configuration Management	Configuration Management
PA 22 Training	Organizational Training
PA 15 Quality Assurance and Management	Process and Product Quality Assurance
PA 21 Process Improvement	Organizational Process Focus
PA 18 Measurement and Analysis	Measurement and Analysis

Work Environment Process Area *

Goal: **A work environment that meets stakeholder needs is established and maintained.**

Practices:

- **Determine work environment needs:** Establish and maintain the needs and requirements to implement, operate and sustain work environments.
- **Establish work environment standards:** Establish and maintain a description of work environment standards and tailoring guidelines that meet identified needs and requirements.
- **Establish work environment:** Establish and maintain a work environment, tailored from the work environment standards, to meet the specific needs.
- **Maintain the qualification of components:** Maintain the required qualification of work environment components.
- **Maintain the qualification of personnel:** Assure that personnel have the required competencies and qualifications to access, use, and maintain the work environment.
- **Maintain technology awareness:** Monitor, evaluate and insert, as appropriate, new technology for improving the work environment.
- **Assure continuity of work environment:**

* NOTE: This is work in progress – see Call for Review package; comments due NLT 1 Mar 2004

Extending CMMI® and iCMM® for Safety and Security: The Way Ahead

- Pilot appraisals have been initiated
  - Two in FAA, one in Lockheed Martin, one may be initiated in Department of Energy
  - These are ARC Class C appraisals, for validation of practices
  - Appraisal feedback will be incorporated
- Final packaging
  - Safety and Security Assurance Application Area
  - Work Environment Process Area
  - Guidance material
  - Consolidated Glossary
  - Mapping to source material
- Distribution for review
- Revision, Publication, and Use

What will it take to get Safety & Security Assurance incorporated within CMMI to provide requisite criteria for evaluating organizations?

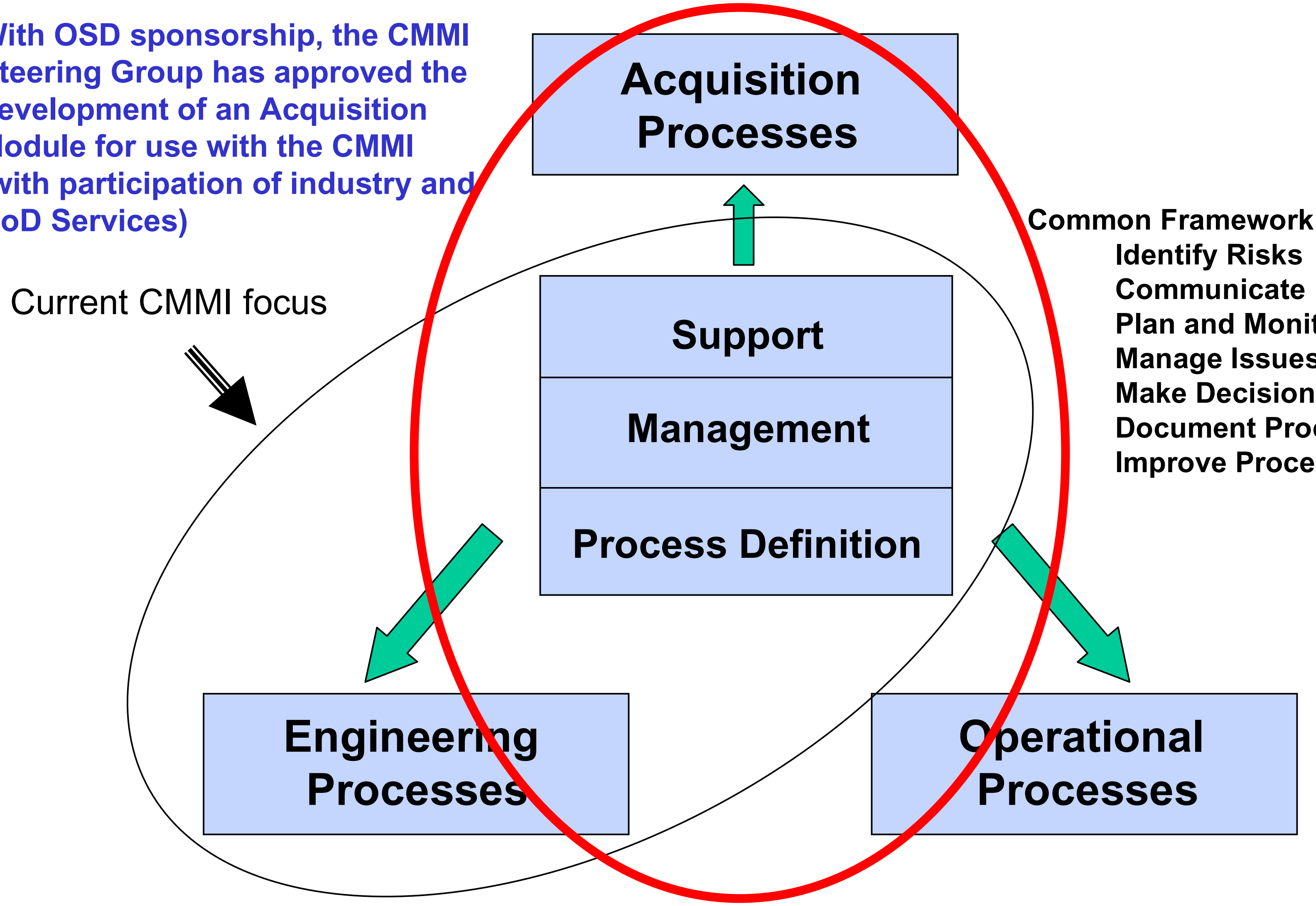
Acquisition use of CMMI & iCMM

- Early warning indicators have been proposed for use in acquisition of software-intensive systems
  - Critical success factors include Goal 2 – “Systems and software acquisition strategies are appropriate and compatible”
    - 2.3. They identify the most critical system and software risks and an effective risk management process
    - 2.4. They are compliant with policy, legal and regulatory requirements, standards, and security requirements

- Acquisition organizations can use the CMMI to:
  - Help discriminate between offerors during a competitive source selection
  - Help encourage contractors to use effective practices and improve those practices after contract award
  - Establish an acquisition process improvement program within the program office
  - Establish a Safety & Security Assurance program for system lifecycle

CMMI & iCMM Provide a Common Framework to Manage Complexity

With OSD sponsorship, the CMMI Steering Group has approved the development of an Acquisition Module for use with the CMMI (with participation of industry and DoD Services)



Common Framework To:

- Identify Risks
- Communicate
- Plan and Monitor
- Manage Issues
- Make Decisions
- Document Processes
- Improve Processes

Safety & Security Assurance Application Area addresses lifecycle risks

Focus for Software Assurance:
Countering Risks for Untrustworthy Software

- **WG1 Security Process Capability Evaluation**
  - Criteria for mitigating risks associated with development capabilities required to deliver secure software
  - Safety & Security Assurance extensions to CMMI & iCMM
- **WG2 Software Product Evaluation**
  - Criteria for independent evaluation of SW products
  - Considerations for federated High Assurance Software Lab
- **WG3 Counter Intelligence (CI) Support**
  - CIFA support to acquisition programs
- **WG4 Acquisition/Procurement and Industrial Security**
  - Legal and contracting considerations for use of CI information
  - Considerations for security criteria for COTS software and SIS acquired through defense acquisition/development programs
- **WG5 User Identification of Protected Assets**
  - Criteria for identifying assets that require ‘high assurance’ software

Software Assurance Program Working Groups -- Leveraging Activities

- **Software Product Evaluation (SPE)**
  - Beyond Defense-wide Information Assurance Program (DIAP)
  - Criteria for independent evaluation of SW products
  - Considerations for federated High Assurance Software Lab
  - Initially, the SPE took immediate action and identified malicious code within shrink-wrapped software products as a major problem area in the malicious code risk category.
    - The SPE team evaluated the problem; identified currently available tools and techniques for addressing the problem; identified gaps and expressed concerns regarding these tools and techniques; identified what is needed to close the gaps; and suggested future directions for further investigation, research or action related to this specific problem.
    - This problem, the evaluation process, and the results achieved to date are discussed in greater detail in SPE WG paper.

Software Product Evaluation WG

“Technical Response for Inherent Software Product Evaluation” Paper

Software Product Evaluation (SPE) Focus Area
Statement of the Problem
Types of Malicious Code
Attacker Attributes
Reasons for an Attack
Implanting Malicious Software
Difficulties in Detecting Malicious Code
Malicious Code Categories
Detection in the First Category
Detection in the Second Category
Deeper Problems
Analysis Scenarios
Current tools and techniques for addressing the problem
Gaps and concerns regarding current tools and techniques
What is needed to close the gaps and address the concerns
Future direction

Software Product Evaluation WG

- SPE working group will coordinate with the GIG Governance structure to identify risk areas, actions currently underway, recommended near-term actions with high potential payoff, and areas for research related to software product assurance within the GIG architecture.
  - Currently identified risks include malicious code; internal or external attacks on GIG backbone, sub-network operations, the core enterprise services, a particular application, or on data; ineffective access control; ineffective compromise recovery; or on-line software or patch distribution mishaps.
  - Another major risk area is the interplay between network, system, and application components as they are hosted in a heterogeneous environment for the first time.
- SPE efforts will identify risks not only with deployable products but also with software development tools.
  - Such tools may include compilers, database management systems and associated products, modeling and simulation tools, code generation tools, requirements management tools, configuration management tools, etc.
  - It is anticipated that, as risks are identified, problem areas that have an impact across the broadest spectrum of the GIG will be targeted for immediate evaluation and action.

Software Product Evaluation WG

- Several short-term opportunities exist to work within the mission area governance infrastructure and with the Program Managers for key DoD programs to ensure the SPE efforts are focused on critical issues, leverage efforts that may be underway within existing programs, and that provide the greatest return on investment.
  - The business mission area has a defined governance strategy with 6 domains defined. Within each domain, opportunities to consolidate programs into net-centric capabilities that leverage COTS to the greatest extent possible and to terminate legacy programs are being identified and taken.
  - The enterprise infrastructure mission area is currently developing a governance strategy. Even as the governance is being developed, opportunities exist for the SPE to work with the three major programs identified under the transport domain and the Network Centric Enterprise Services (NCES) program that will provide the core enterprise services.
  - The COTS and GOTS products are already defined for some of these programs and will be emerging over the next several years for others. The SPE will focus on the net-centric solutions identified by these mission area and the COTS/GOTS products required to implement those solutions.

Software Product Evaluation WG

- Although SPE efforts are primarily product focused, the SPE will coordinate within the Software Assurance Program and with GIG Governance teams to stress the importance of strong management and process implementations to reduce risks identified and addressed within the SPE working group.
  - The SPE will advocate processes to ensure that only approved software is installed and/or running on the GIG, i.e. strong configuration control of software products and rigorous automated network and system management techniques.
  - The SPE will work with the Software Assurance IIPT outreach to industry to identify opportunities for risk reduction prior to product delivery. Such opportunities may include new standards or improvements to existing standards cited in the JTA. Other opportunities may include the ability to easily enable/disable functions and capabilities within a COTS product.
- The SPE will also track the GIG test-bed activities at NRL. The SPE will assess test results to determine new software assurance risks, identify new problems within existing risk areas, or make recommendations for new research related to software assurance in a net-centric environment.

Software Product Evaluation WG

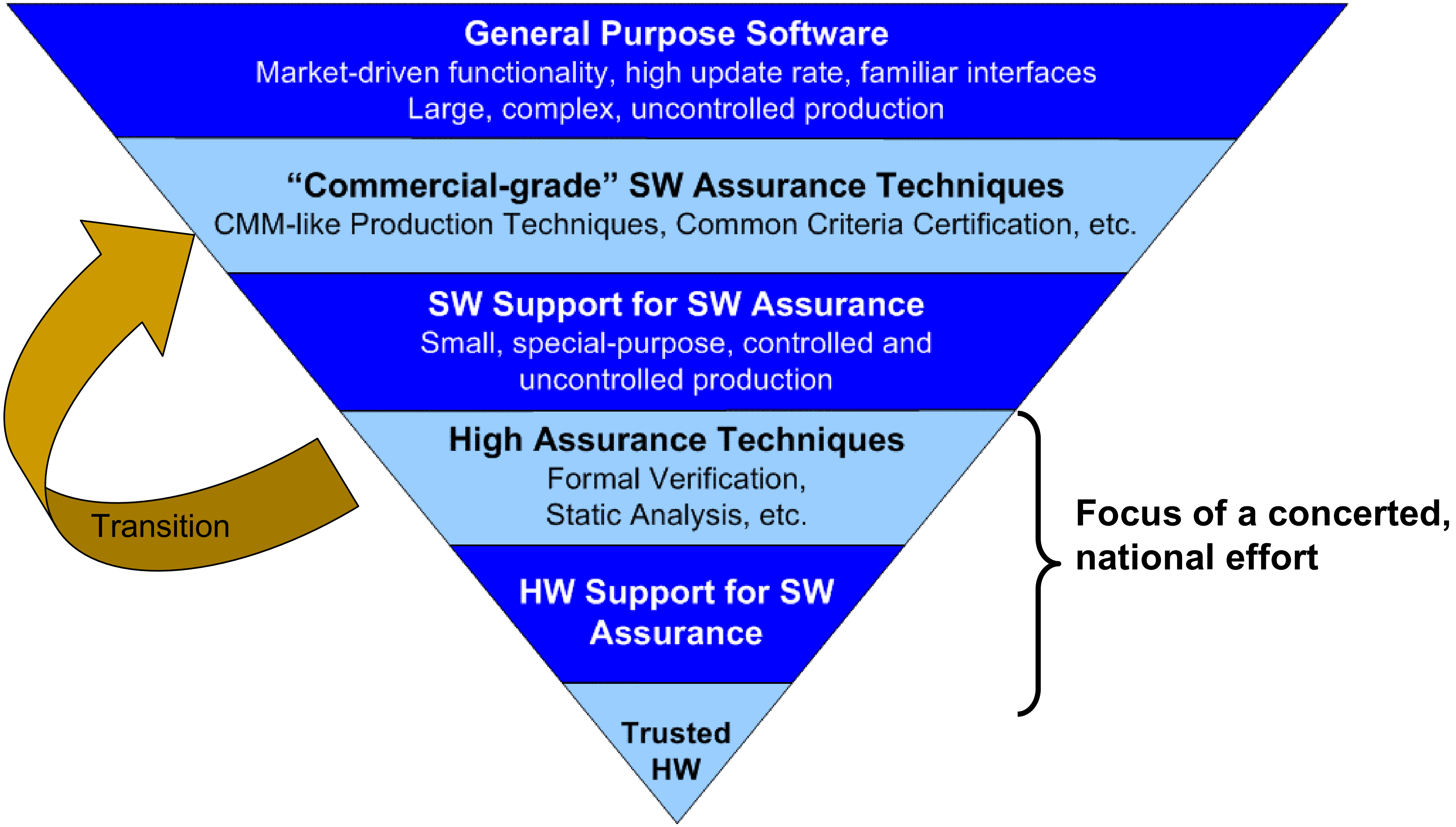
- The SPE may identify opportunities for further research and development.
  - The SPE will work with the DoD research community first to determine if any applicable research is currently underway. For example, the efforts currently underway in the Air Force Research Laboratory (AFRL) Software Protection Initiative may have identified areas for further research.
  - Recent investigations under this effort include research to produce a secure protected development repository and a project to focus on the protection of software from reverse engineering. SPE is taking steps to gain further information on the current status of these efforts.

- Other potential research efforts, for example, may include the need to initiate research, as the trend to make software components more readily available, into the ability of a user to assemble a unique application from multiple component parts in real-time.
  - Such a capability would be a natural follow-on to the enable/disable of COTS product components but it also may introduce new risks into net-centric environments.

Software Assurance Program Working Groups -- Leveraging Activities

- **Counter Intelligence (CI) Support**
  - CIFA support to acquisition programs
- **Acquisition/Procurement and Industrial Security**
  - Legal and contracting considerations for use of CI information
  - Considerations for security criteria for COTS software and SIS acquired through defense acquisition/development programs
- **User Identification of Protected Assets**
  - Criteria for identifying assets that require ‘high assurance’ software

How will we build this assurance?



General Purpose Software

Market-driven functionality, high update rate, familiar interfaces

Large, complex, uncontrolled production

“Commercial-grade” SW Assurance Techniques

CMM-like Production Techniques, Common Criteria Certification, etc.

SW Support for SW Assurance

Small, special-purpose, controlled and uncontrolled production

High Assurance Techniques

Formal Verification,
Static Analysis, etc.

HW Support for SW Assurance

Trusted HW

Transition

Focus of a concerted, national effort

Concepts presented through collaboration of John Hopkins University Applied Physics Lab with DoD

High Assurance Software Lab Components

- High Assurance Research Institute
  - Define the end-to-end problem space
  - Sponsor/collaborate on research into dark areas
  - Conduct classified research
- High Assurance Software Foundry
  - Apply design assurance techniques to produce special products needed for end-to-end high assurance
- High Assurance Engineering Center
  - Analyze target SW products
  - Re-engineer, supplement as needed
  - Certify SW products for use – policy definition

Concepts presented through collaboration of John Hopkins University Applied Physics Lab with DoD

The Way Forward
(near term)

Collaboration will continue and more stakeholders are being invited to participate

- 2-3 Feb – Information Assurance Workshop, Atlanta
- 12-13 Feb - Software Assurance Forum at IDA, Alexandria
- 27 Feb – Interim Report with findings & recommendations
- 1 Mar – Deadline for Review Comments on Safety & Security Assurance Application Area
- 31 Mar – Report to Dept of Homeland Security on "Securing Software"

Observations

- Industry has invested in process improvement for at least 15 years
  - Emphasis shifting to system engineering as well software engineering
  - Incentives for delivering trustworthy software dwarfed by other business objectives
- Pivotal momentum gathering in Government’s recognition of (and commitment to) process definition and improvement in its acquisition, management and system engineering activities
  - 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 security perspective, acquisition and development practices should only be categorized as “best practices” if they also contribute to the delivery of systems that are safe and secure.
  - Qualification of software products and suppliers’ capabilities may be some of the more important risk mitigation activities of acquiring organizations
  - A federal focus is needed to achieve objectives of high assurance software

Contact Information

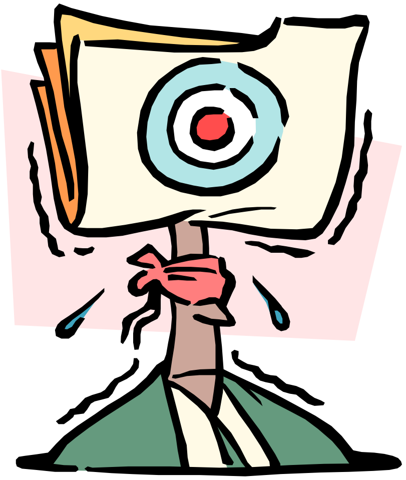
Joe Jarzombek, PMP

Deputy Director for Software Assurance
Information Assurance Directorate
Office of the Assistant Secretary of Defense (NII)

Business Ph (703) 604-1489 x154
Mobile Cell Ph (703) 627-4644

Joe.Jarzombek@osd.mil

Crystal Gateway 3, Suite 1101
1215 Jefferson Davis Highway
Arlington, VA 22202-4302



Selected terminology - 1

RELATED DEFINITIONS (extracted from consolidated Safety/Security Glossary)

Assurance argument: A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

Integrity Level: A denotation of a range of values of a property of an item necessary to maintain system risks within tolerable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.

“The system integrity level corresponds to the tolerable level of risk that is associated with the system. A system can be associated with risk because its failure can lead to a threat, or because its functionality includes mitigation of consequences of initiating events in the system’s environment that can lead to a threat.”

Software safety integrity: Measure that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time

Software safety integrity level: Discrete level (one out of a possible four) for specifying the safety integrity of software in a safety-related system

Selected terminology - 2

Risk: Combination of the probability of occurrence of harm and the severity of that harm; The combination of the frequency, or probability, and the consequence of an accident; An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability; The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

Threat: A state of the system or system environment which can lead to adverse effect in one or more given risk dimensions; The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability; Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or a system.

Threat analysis: The examination of threat-sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy; includes a weakness of an asset or group of assets which can be exploited by a threat

Hazard: Potential source of harm; A physical situation, often following from some initiating event, that can lead to an accident; A condition that is prerequisite to a mishap.

Hazard probability: The aggregate probability of occurrence of the individual events that create a specific hazard.

Hazard severity: An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

Availability of “Qualified” COTS

- On Dec 24, 2002, the Deputy Secretary of Defense approved Management Initiative Decision (MID) 905, “Net-Centric Business Transformation and E-Government”
- On Apr 8, 2003, DoD CIO approved the COTS IT/ National Security Systems (NSS) Software Action Plan as a roadmap of near-term initiatives that begin to execute this vital transformation.

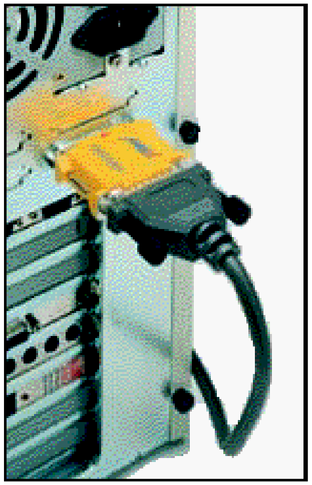
New Paradigms for Defending Critical Information Resources

- Changes in practices are necessary, but insufficient; technology must also be inserted.
- New paradigms are needed to defend critical information systems against sophisticated and well-resourced adversaries such as terrorists and nation-states.
  - DARPA’s OASIS program is designed to meet these challenges.
  - OUSD(AT&L) DDR&E-sponsored Software Protection Initiative is designed to ensure technology and policy protection measures are appropriately applied, balancing mission requirements with security

Software Protection Initiative

Goals

- Slow the acquisition of DoD applications software by our adversaries
- Make cost-prohibitive the exploitation of DoD software when it does “leak”
- Ensure that technology and policy protection measures are appropriately applied, balancing mission requirements with security

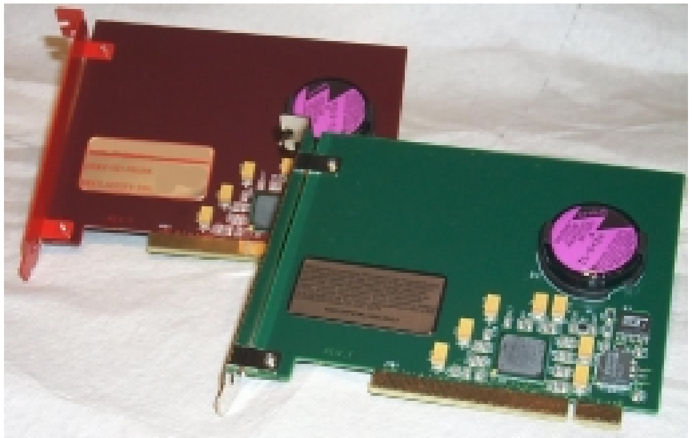


Commercial Approaches
• Encrypted executables
• Node-lock software
• Dongles

Good for revenue protection

Not adequate for ITAR software

NEED STRONGER PROTECTIONS!



XPATCH Cards

Congressional interests about software security requirements

Recent Congressional interests relative to 2004 provisions that have raised questions about software security requirements?

- urge implementation of an "architecture or blueprint" for all DoD IT systems (the architecture or blueprint is to protect against unauthorized modifications or insertions of malicious code into critical software and against "reverse engineering" of intellectual property within that software). *

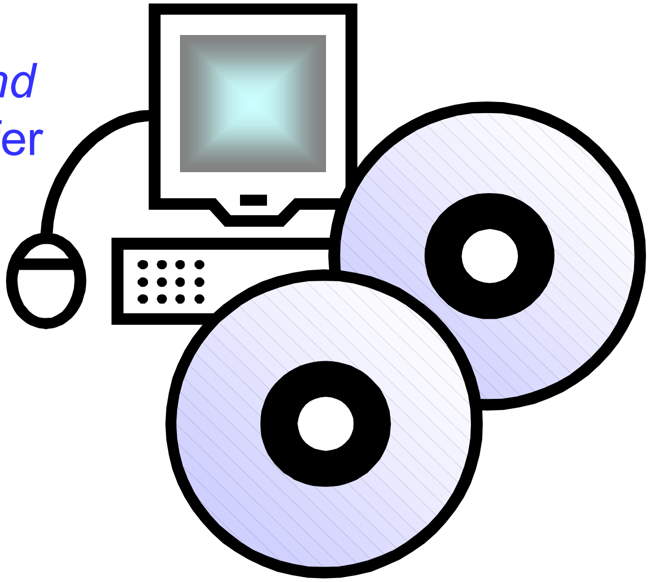
- direct DoD to assess the usefulness of tamper-resistant security software and other security tools (it says tamper-resistant software inserts "security-related functionality directly into the binary level of software code").

* One provision calls for DoD to ensure that its recent emphasis on using COTS software will not make sensitive command, control, communications and intelligence for Defense more vulnerable. The measure says the department "must be more proactive" in protecting its information systems and urges implementation of an "architecture or blueprint" for all of its information technology systems.

Definitions

Information Systems:

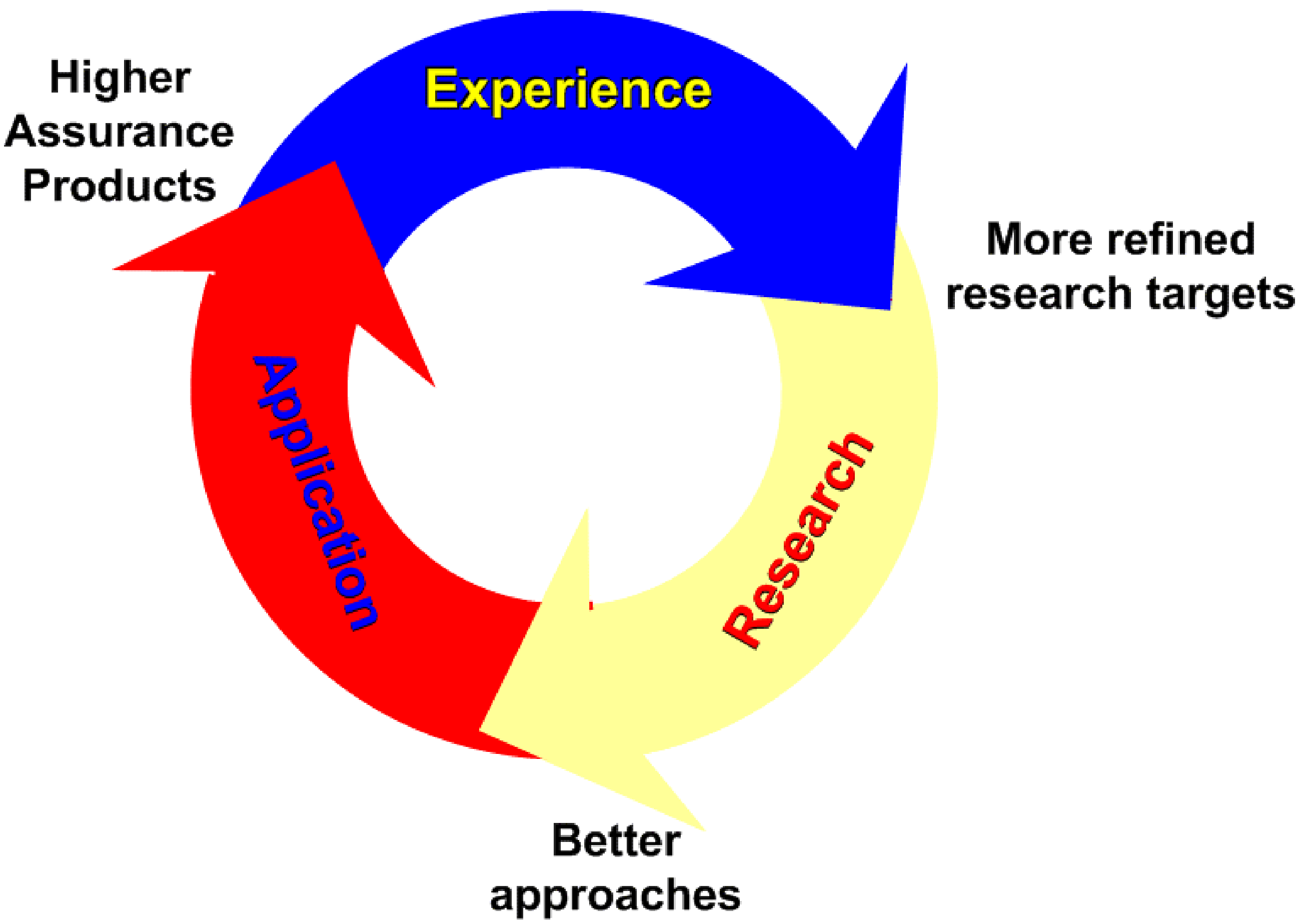
Complex compositions of *hardware and software* that process, store and transfer information.



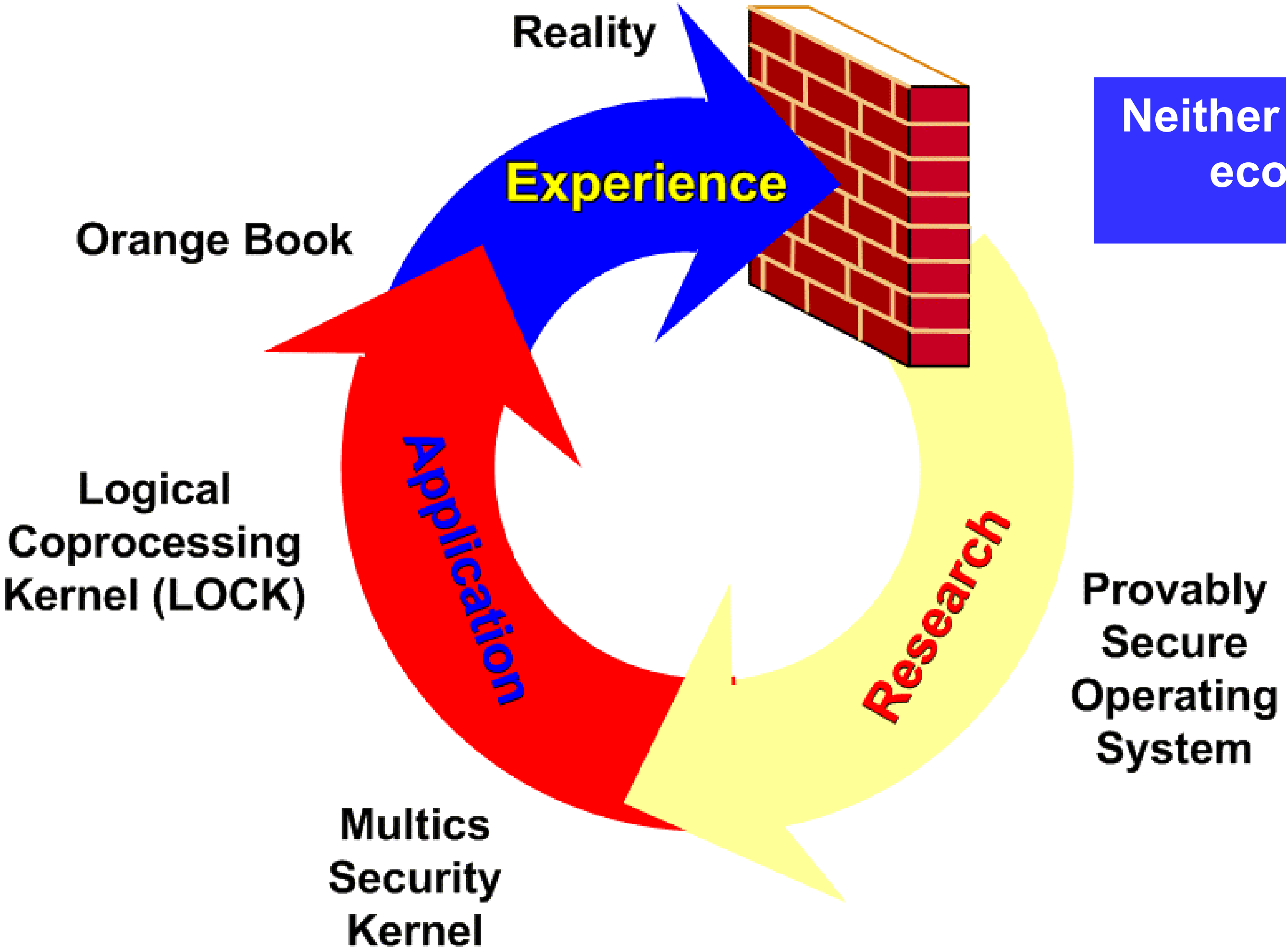
High Assurance Information Systems:

Information systems that we <u>know</u> will do* what we want *them to do, and* only what we want *them to do.

The Classic Approach

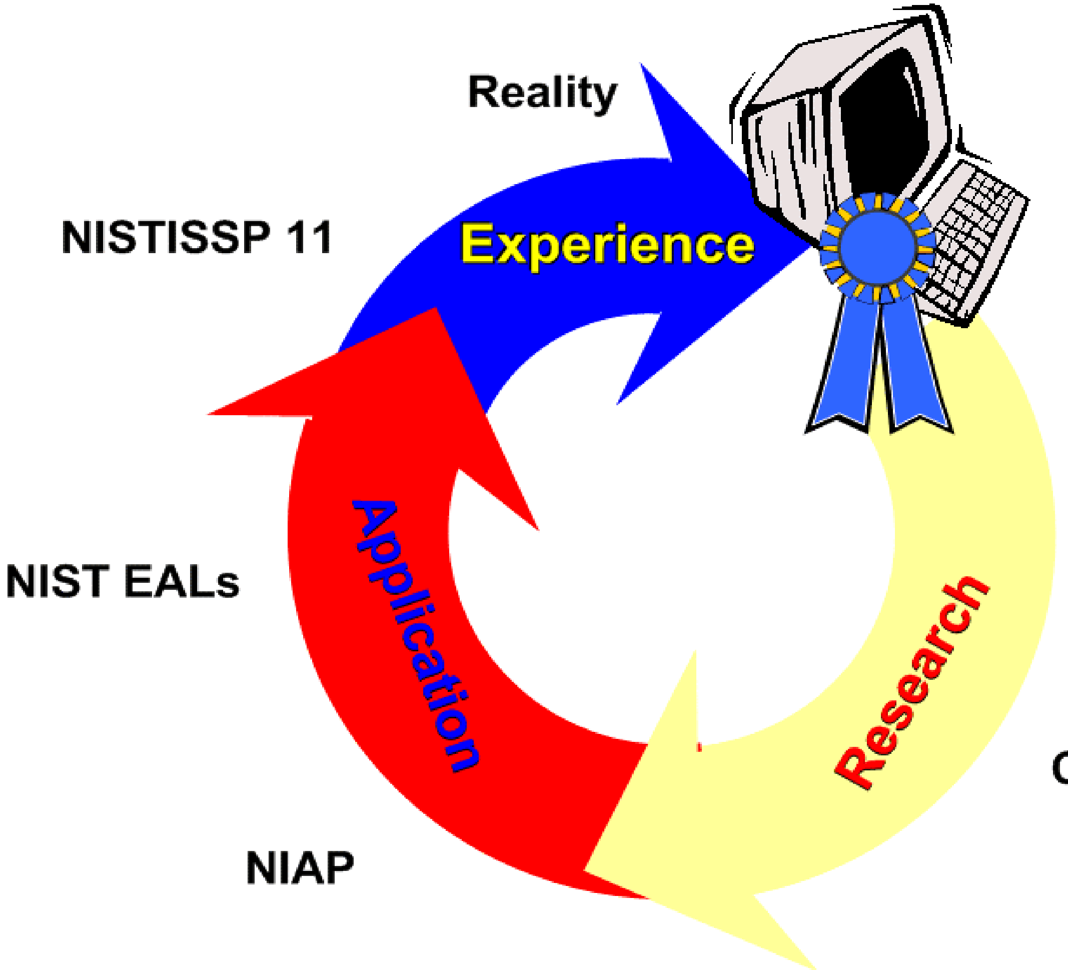


First Time Around the Track



Neither timely nor economic

Second Time Around the Track



Burdens vendors without providing security

We must carry these lessons forward!

Lessons Learned

COTS software is, and will remain, a part of our secure systems

- – GOTS cannot match COTS development speed or cost

+ We cannot mandate security standards we won't wait or pay for
+ Market forces overwhelm our influence on vendors
  - – Drive for market share precludes use of time-consuming high assurance techniques
+ The design assurance paradigm (alone) may be unworkable
  - – Cannot control vendor design and test methods

A national problem requiring a national commitment

We need research into the hard problem of understanding and using commercial systems as they come to us.

A Significant Research Base.......

Academia *	Industry *	Government
Carnegie-Mellon	*ARCA*	*National Institute of Standards & Technology*
Drexel	*Citigal, Inc.*	*National Security Agency*
JHU	*GammaTech, Inc.*	*Air Force Research Lab*
Kansas State U.	*Kestrel Institute*	*Naval Research Laboratory*
MIT	*Microsoft Research*	*Army Research Laboratory*
NYU	*Praxis Critical Systems, Ltd.*	
U. of Arkansas at Little Rock	*SRI, Inc*	
University of MD	*SoHaR (Software and Hardware Reliability)*	
University of Oregon	*Telos / Xacta*	
University of Texas		
Vanderbilt		

* Representative sampling in alphabetical order

A Handful of Research Topics….

Aspect of High Assurance	Research Approaches
Building What We Want	Formal Specification Methods Formal Verification Methods High Assurance Process Definition Automatic Code Generation from Formal Designs Higher-Order Type Languages
Understanding What We Built	Assurance Evidence Presentation Decompilers & Dissassemblers Static Source Code Analysis Program Slicing for Program Understanding Testing for High Assurance Testing for Security Properties Automated Test Generation from Formal Specifications
Using What We Understand	Composable Security Architectures Verification of Security Policy by Formal Methods

A Number of "Research Coordinating" Bodies….

- High Confidence Software and Systems
  - Provide a sound theoretical, scientific, and technological basis for assured construction of safe, secure systems.
  - NSA, NIST, DARPA, NSF, FAA, NASA
- Technical Cooperation Program (TCCP) – Group "S" Technical Panel (STP)-11
  - Technology for … security of specific applications of high military interest
  - US, UK, Canada, Australia, and New Zealand
- Infosec Research Council
  - Identify high priority areas of research.
  - DARPA, NSA, OSD, AFRL, AFIWC , ARL, CECOM, NRL, ONR, SPAWAR, CIA, NRO, DOE, FAA, FBI, NIST, NRC, and NSF

Some Major Research Programs…

NRL – Center for High Assurance Computer Systems **Improved methods for [creating] and certifying computer systems that must enforce security requirements, including use of formal methods**	***Software Cost Reduction:*** **Formal methods for specifying and verifying software requirements**
DARPA/ATO Composable High Assurance Trusted Systems **Provide the high assurance trusted operating systems context/basis to host the planned security services needed to … secure highly distributed mission critical information systems for the DoD.**	***MOdelchecking Programs for Security properties (MOPS):*** **Compile-time checking of C programs for temporal safety properties (UC Davis)**
CMU/SEI **Structured method for designing high assurance systems**	***Flow-Service-Quality (FSQ) Requirements Engineering for High Assurance Systems:*** **Structured design Methodology**
NIST High Integrity Software Systems Assurance **Provide technology to produce high integrity, affordable software in high integrity software systems**	**Automated Test Generation from Formal Specifications**

Research Shortfalls

- Inadequate coverage of the problem space
  - Lofty goals; handfuls of projects
  - Specific languages, fault types & application types
  - No single thread; no vertical integration
- Focus
  - Focus on high assurance software *development*
  - *Development* may never be under our control
  - *Reliability* focus dilutes progress towards *assurance* goals
- Urgency
  - Spending is completely inadequate to the size and difficulty of the problem

Shortfalls in Practice

- Scattered Efforts
  - National Security Agency
    - More opportunity than is strictly desirable!
  - Sandia
  - Joint Interoperability Test Command
    - Code Assessment Vulnerability Analysis (CAVA) Methodology
  - Naval Security Group at Pensacola, FL
    - Inspection of GOTS software
- Little communication or sharing of results
- Few ties to the research community

Lessons Learned

Independent researchers don't produce end-to-end solutions

+ Research coordinating bodies don't produce end-to-end solutions
  – Researchers will study what appeals to them
+ The problem is much larger than the amount of resources allocated to it
  – Needs sustained, coordinated efforts
+ We learn by DOING
  – Practice forces and hones theory

Can't wait for a breakthrough from independent research

We need a concentrated, sustained effort to tackle real problems

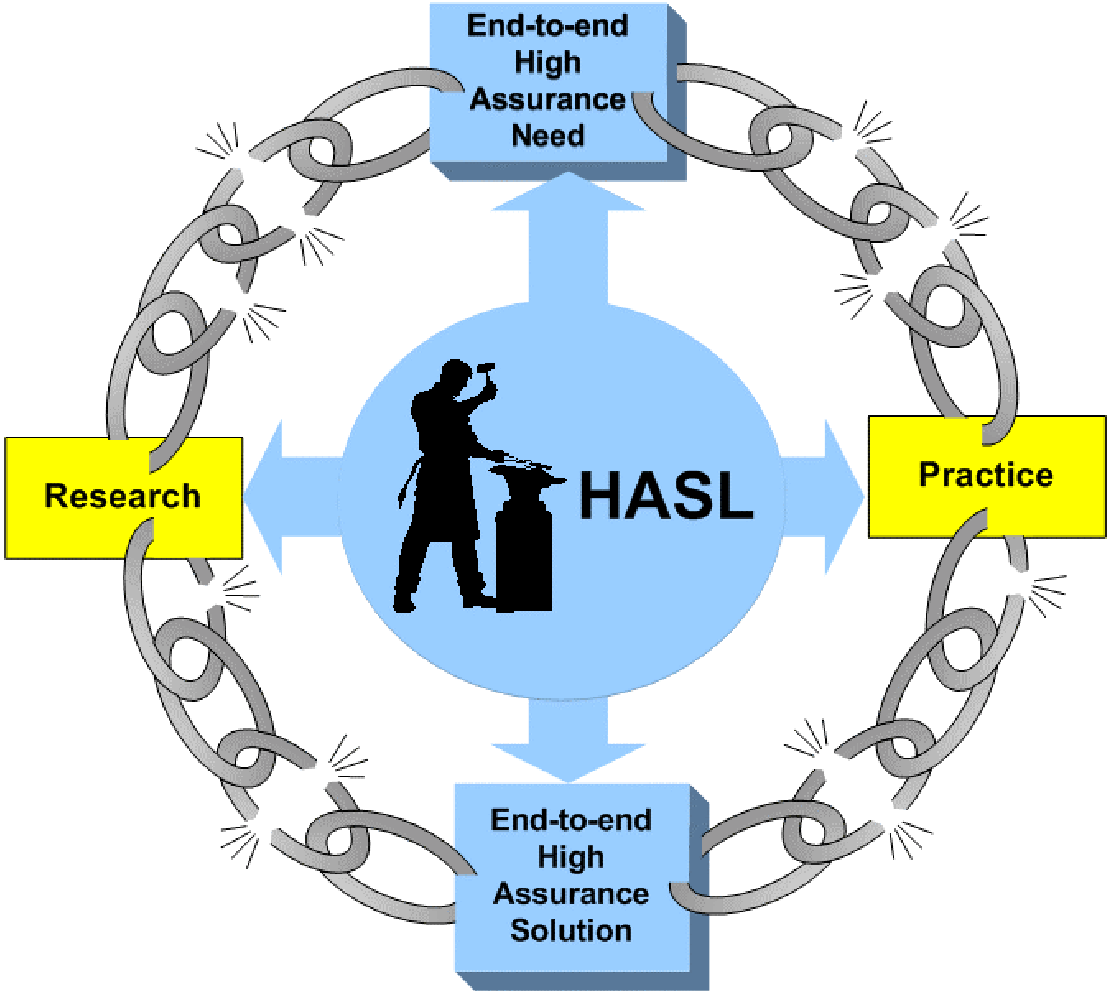
National High Assurance Software Laboratory (HASL)

Mission

To develop the capability to protect the United States Government from malicious software by:

- Focusing research to create end-to-end solutions
- Serving as a bridge from research to practical application
- Certifying selected COTS/GOTS software products for particular uses
- Creating selected software products needed for end-to-end solutions

HASL Forges the Missing Links



End-to-end High Assurance Need

Research

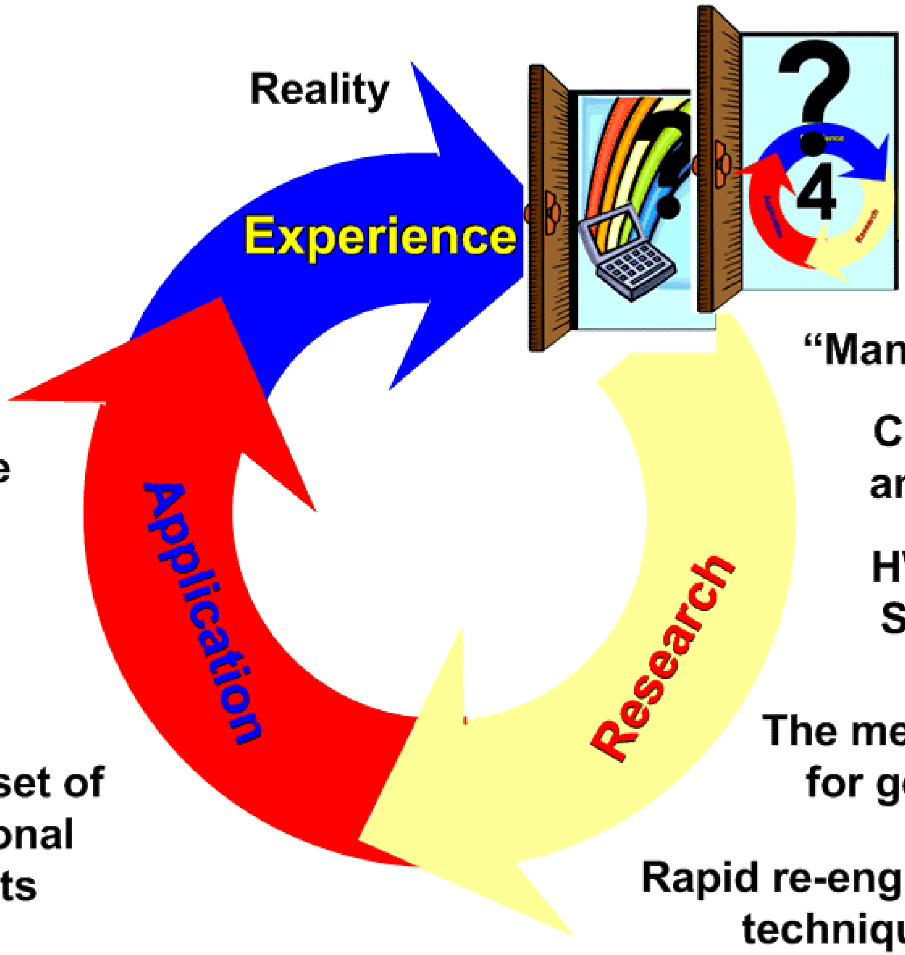
HASL

Practice

End-to-end High Assurance Solution

A Third Time Around?

We will learn until we solve this problem.



Reality

Assurance products

Minimum set of foundational products

“Manhattan Project” funding

Coexistence of trusted and untrusted systems

HW support for SW assurance

The meaning of certification for general purpose SW

Rapid re-engineering techniques

Metrics

What DoD & DHS Must Do

- Lead the education of national leaders on the scope and seriousness of the problem
  - What we know has happened
  - What we know is possible
  - Define the “Einstein letter” of high-assurance software
- Promote the formation of a national laboratory that can address this problem
- Demonstrate approaches that work
  - Build the nucleus around which the Laboratory will form
  - Develop new paradigms
  - Bridge the gap between research and application

Identify Lead Agency

Demonstrate the Solution

- Create a blueprint for the National High Assurance Software Laboratory
- Plan and implement a skeleton Laboratory
  - Demonstrate feasibility
  - Build relationships
  - Solve some immediate problems

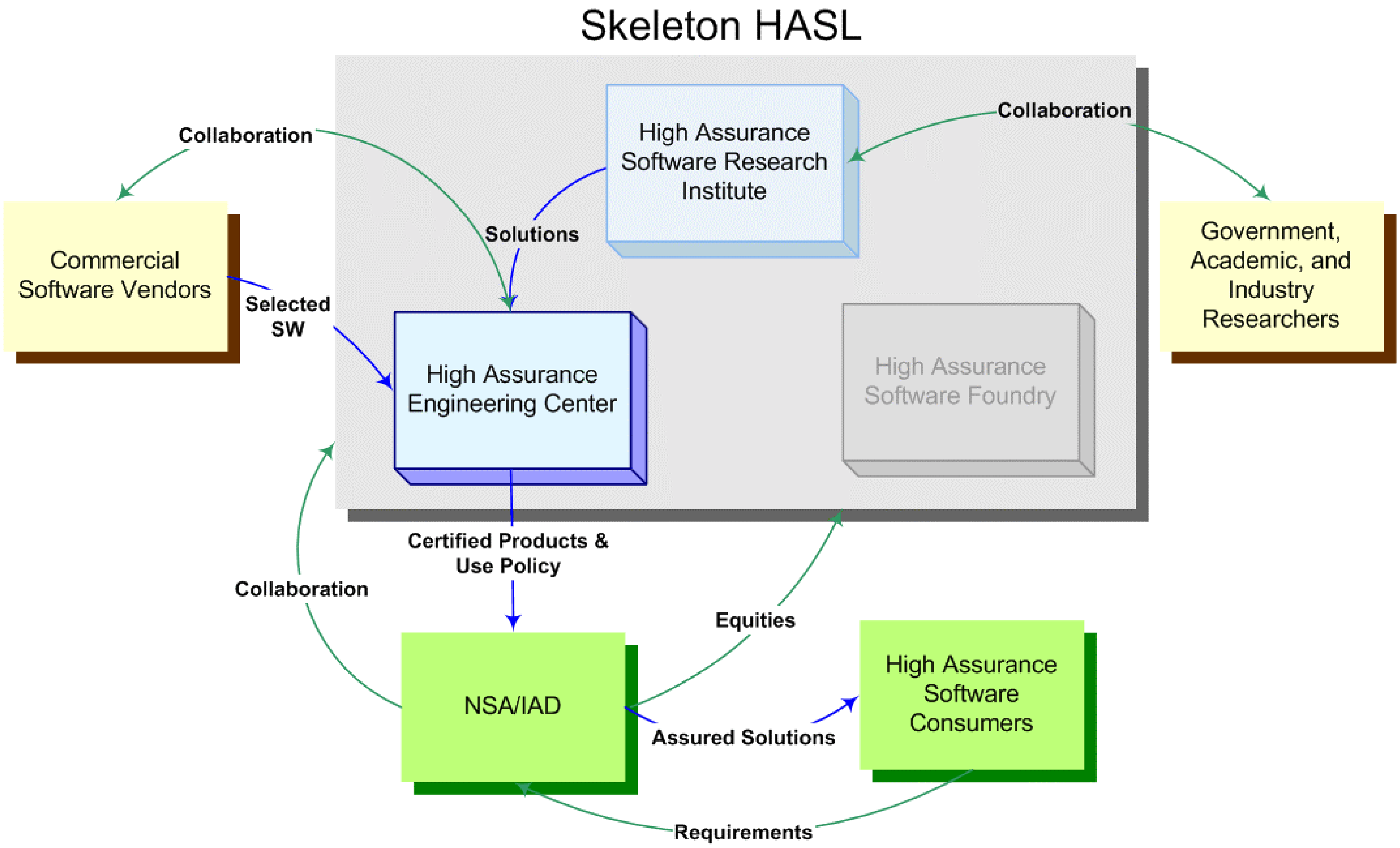
Attributes of the National HASL

- Tightly coupled research and application of research activities
  - Engineering high assurance from industry-produced software
  - Create GOTS software for special applications
- Collaboration by government, industry and academia
  - Provide neutral ground with intellectual property protection
  - Formal agreements on rights to results
- Focus on national needs
  - Requirements of government high-assurance software consumers
  - Equities

Concept of Operations

- Core staff of administrators, framers, researchers and practitioners
  - Core staff may alternate between researchers and practice
- Sensitivity-based, multi-tiered staff, facilities and activities
- Core researchers augmented by collaboration with industry and academia
  - Off-site partnerships
  - Fixed-term, on-site research positions
- Core evaluation practitioners augmented by collaboration with vendors
  - Fixed-term, on-site positions
  - Expertise for specific product evaluations

The Skeleton Laboratory


Skeleton HASL
High Assurance Software Research Institute
Collaboration
Collaboration
Commercial Software Vendors
Solutions
Selected SW
Government, Academic, and Industry Researchers
High Assurance Engineering Center
High Assurance Software Foundry
Certified Products & Use Policy
Collaboration
Equities
NSA/IAD
High Assurance Software Consumers
Assured Solutions
Requirements