The Department of Defense (DoD) and Software Assurance

Larry Wagoner
March 9, 2005

DoD and Software Assurance

- What is the problem?
- Why is Information Security so hard?
- What are the software market trends?
- What is the threat?
- What is the DoD response to this problem?

Software Assurance

Goal: Mitigate risks attributable to software exploitation in critical software by untrusted & undisciplined developers:

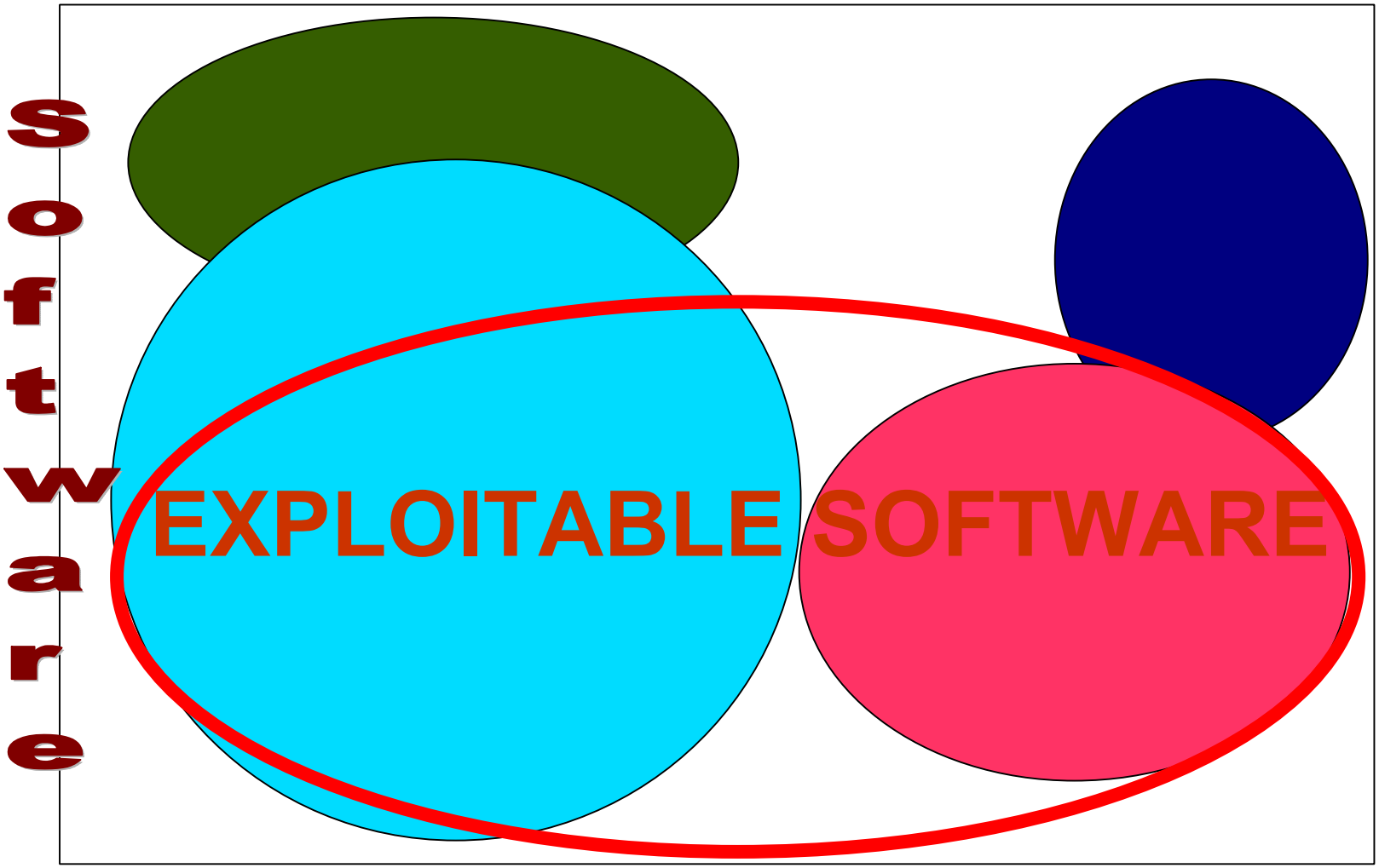
- eliminate malicious code
- reduce software vulnerabilities

Software Assurance: "The level of confidence that software is free of exploitable vulnerabilities, either intentionally designed as part of the software or accidentally inserted, and that the software functions in the manner as would be expected by a customary user."

[Source: Interim Report on "Software Assurance: Mitigating Software Risks in the DoD IT and National Security Systems," DoD OASD(NII), Oct 2004]

Exploitable Software -- Conceptual Perspective:
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

- Not all defects are exploitable vulnerabilities and not all vulnerabilities are defects

The Software Assurance Problem

- **Critical systems are dependent on sophisticated software**
- **Insufficient assurance in the security & reliability of commercial software.**
- **Increasing reliance on commercial software**
- **Consequence of vulnerable software:**

Software is exploited =>

System fails =>

Mission fails

Why Information Security is Hard

- Three influencing features of IT markets
  - Value of a product to a user depends on how many others adopt it (Metcalfe's law)
    - E.g. telephones, credit cards, the Internet, HDTV
  - Technology has high fixed costs and low marginal costs
    - So do airlines, hotels, stadium events
    - Price should be driven down to the cost of production
  - Often large costs to users to switch technologies
    - Leads to lock-in
- Extremely important to get products to market quickly
  - Economic drivers will not support security

Software Trends

- Business factors drive functionality rather than security
- Commercial software is extremely, and increasingly, complex
- Software pedigree is often unknown (and unknowable)
- Time to custom develop software for critical systems is too long
- Cost to custom develop software for critical systems is prohibitive

Current Software Market Trends

- 25% of IT jobs to be outsourced to developing countries by 2010
- 15% of US IT projects over the next 5 years to be done in India
- Offshore IT outsourcing market to grow at a rate of 20% per year
- India is the current leader; China and Russia emerging quickly
- R&D outsourcing may be next trend

The Threat to DoD

- DoD is a target
- Risks due to exploitable vulnerabilities, whether unintentional or intentional, are real
- Foreign influence into commercial software is substantial
- Ample foreign opportunity to implant malicious code
- Malicious coder could be anywhere (U.S. or offshore)
- Software can be attacked or exploited at any point in its life-cycle: development, distribution, operational use, maintenance
- Very low level of investment and risk for adversary to implant malicious code

The Farewell Dossier

- Soviets were stealing large amounts of Western technology in the late 1970's/early 1980's
- CIA and DoD modified products were “made available”
  - Contrived computer chips found their way into Soviet military equipment
  - Defective plans disrupted the output of chemical plants and a tractor factory
  - Flawed turbines were installed on a gas pipeline
- Soviets were left to wonder what else was “modified”

National Security Requires Software Assurance

- Software assurance is required to fulfill DoD missions and protect critical infrastructure
  - DoD capabilities dependent on software
  - Reliance on all forms of commercial software by DoD is accelerating
  - Risks of using unvetted software by DoD must be addressed
  - Exploitable vulnerabilities and malicious code place critical capabilities at risk
  - In era of asymmetric warfare, opponents can threaten software-enabled capabilities cheaply and safely

Congressional Interest

FY04 Def Auth Conf Report 108-354, **S*ecurity of Sensitive Software*** --

- DOD must ensure that recent emphasis on procurement of COTS software will not open vulnerabilities in sensitive DOD C3I software

- DoD must provide IA and protection for all DOD IT assets, including:
  - unauthorized modifications to code in mission critical software;
  - insertion of malicious code into mission critical software;
  - reverse engineering of mission critical software.

Responding to 2 Congressional Sub-Committees, GAO Review #120221 resulted in May 2004 GAO-04-678 Report **"Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks"**

- Outsourcing, foreign development risks & insertion of malicious code
- DoD noted domestic development subject to similar risks

Congressional Interest (cont.)

Addressing software issues for all Critical Infrastructure relied upon by Federal Agencies (addressed by several Congressional sub-committees, the GAO has initiated a new consolidated review in Nov 2004.

Congressional Research Study Report, "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, February 22, 2005

- Addressed vulnerabilities attributable to exploitable software

Software Assurance Initiative (SAI)

- OASD (NII)/DoD CIO led Software Assurance Initiative in 2004
- Used Working Groups coordinated by Steering Group
  - Prioritization of Protected Assets
  - Supply Chain Awareness
    - Supplier Threats
    - Supplier Security Process Capabilities

    } (includes Outsourcing)
  - Acquisition/Procurement & Industrial Security Policies
  - Software Product Evaluation (product focused)
  - Workforce Education and Training
  - Research & Development
- Held Forum to gather additional data and vet findings
- Produced interim report, *Software Assurance: Mitigating Software Risks in the DoD IT and National Security Systems*, Oct 2004

SAI Science and Technology Findings

- Finding: There is no focal Point within DoD to develop new diagnostic and evaluation tools to test for assured software, and to coordinate testing standards and testing across the DoD, the National Labs and Centers of Academic Excellence

- Finding: DoD cannot identify software vulnerabilities and mitigate their risks in a timely manner

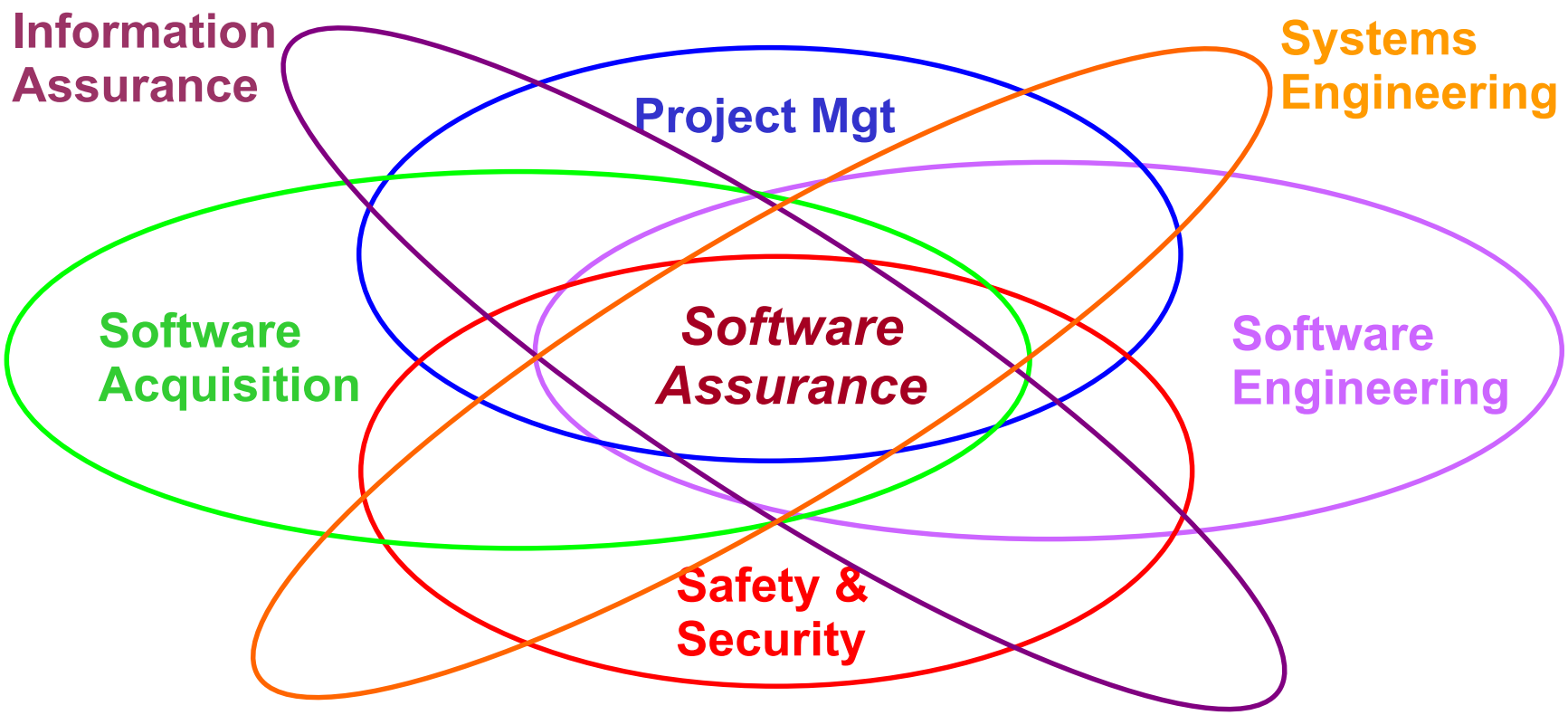
DoD Activity

- DoD is in the process of reviewing the findings and recommendations of the SAI
- Next DoD-DHS Software Assurance Forum
  - 11-12 April, 2005
  - Alexandria, VA
  - https//enstg.com/Signup/default.cfm
  - Conference code: SOF60973
- Workshops
  - Software Tools and Product Evaluation
  - Software Processes and Practices
  - Software Workforce Education and Training

Software Assurance Education & Training

- Teaming with Department of Homeland Security
- Scope workforce needs for SW assurance
  - Knowledge Areas
  - Core Competencies
- Leverage related “best practices” work from universities and standards bodies
- Develop Software Assurance Common Body of Knowledge
- Support development of related curriculum

Interrelationship Among Disciplines Contributing to Software Assurance Body of Knowledge*



* Note: Initial input (subject to update) for the contributing bodies of knowledge (BOK) comes from:

a) IEEE CS SW Eng Body of Knowledge (SWEBOK) for Software Engineering, www.swebok.org
b) PMI Project Management Body of Knowledge (PMBOK) for Project Management, www.pmi.org
c) DAU SW Acquisition Management (SAM) Core Competencies for SW Acquisition, *http://acc.dau.mil*
d) Safety and Security extension for integrated CMMs from 8 S&S standards & ISSE, *www.faa.gov/ipg*
e) DoD Information Assurance Training, Certification and Workforce Management, DoD 8570.1-M
f) DoD Systems Engineering, http://www.acq.osd.mil/ds/se/index.html

Interrelationship Among Disciplines

- From an Education and Training perspective, Software Assurance could be addressed as:
  - A “knowledge area” extension within each of the contributing disciplines;
  - A stand-alone Body of Knowledge drawing upon subsets of the contributing disciplines;
  - A set of functional roles, drawing upon a common body of knowledge; allowing more in-depth coverage dependent upon the specific roles.
- Curriculum could be developed based on the common body of knowledge or functional roles

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
  - Resource constrained
  - Need to influence R&D

R&D – Research and Development

- Top Priorities
  - Cost-effective, improved source scanning, correct by construction
  - Composability of secure systems
  - Improved binary scanning tools
  - Trustworthy computing base
  - Minimize/control functionality
  - Metrics and measurements of exploitability
  - Detect/counter run-time vulnerabilities
- Groupings
  - Development processes
  - Scanning/detection of vulnerabilities
  - Countermeasures
  - Development tools
  - Application Environment
  - Requirement/Design/Validation
  - Education and Training
  - Secure Kernel

All

High Assurance

Less than High Assurance

Government Perspective of Software Assurance

- Significant government/industry interest in SW assurance
- Continue to leverage all sources of software, but reduce risk
  - Raise level of trust for all software
  - Minimize vulnerabilities and understand threat

- DoD in conjunction with DHS is identifying and specifying SW Assurance processes/practices and SW-enabled technologies to mitigate risks
- Software Assurance body of knowledge should be delineated to support education and training, and lifecycle management
- Continue collaboration with industry / academic institutions

The End.

Larry Wagoner

l.wagone@radium.ncsc.mil