Overall Classification of This Briefing is:
UNCLASSIFIED

SELinux Symposium:

An Annual Exchange of Ideas, Technology and Research Involving SELinux

Mr. Daniel Wolf

Information Assurance Director

March 2005

Agenda

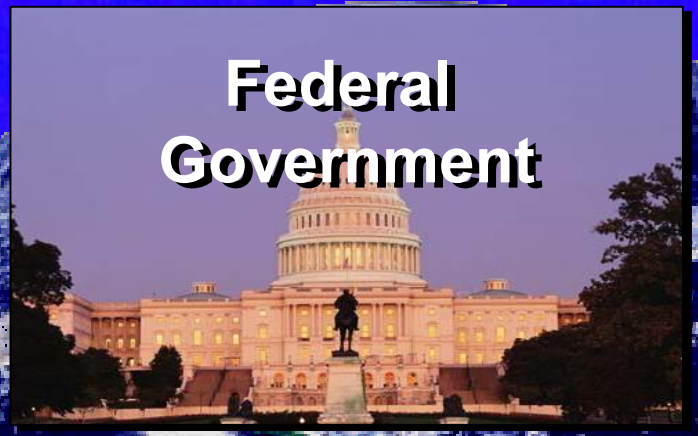
- IAD Mission
- COTS Strategy
- Software Assurance
- NSA Security-Enhanced (SELinux)
- Common Criteria

IAD Mission

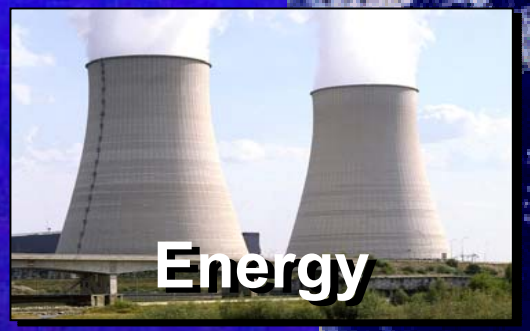
- In the face of sophisticated global attacks against America, we provide customers the knowledge, technology and assistance they need to enable their missions and to assure their information systems.

- applying the five tenets of information assurance
  - Availability
  - Integrity
  - Authentication
  - Confidentiality
  - Non-repudiation


Finance


Federal
Government

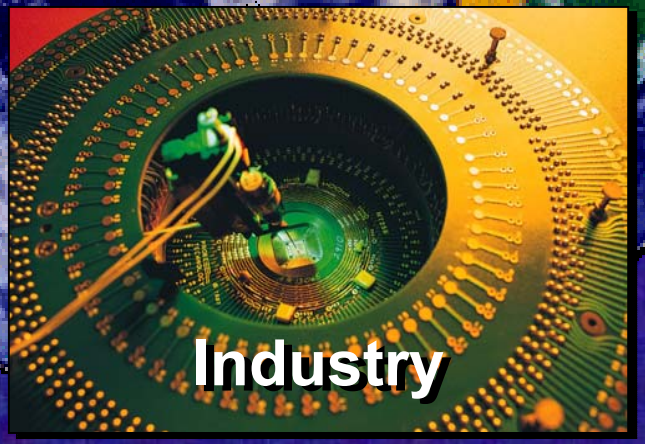

Transportation

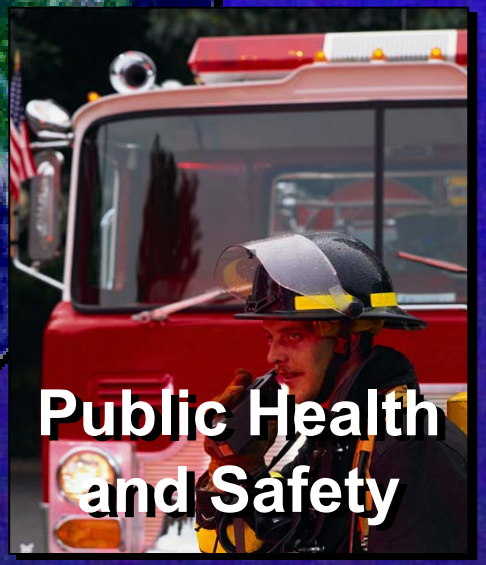

Energy


National Security
Intelligence/DoD


Water


Telecommunications


Industry


Public Health
and Safety

Discover Vulnerabilities

Generate & Develop Solutions

Deploy and Maintain Solutions

IAD Business Lines

Conduct Defensive Information Operations

Conduct Research

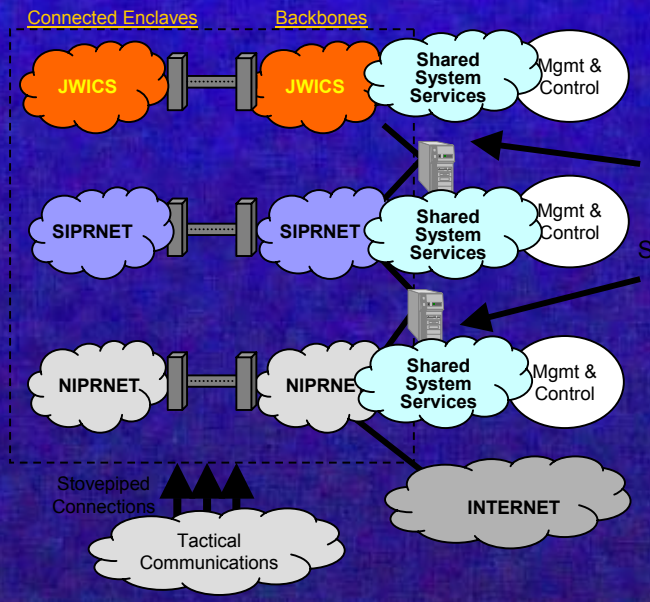
Design and Build Special-purpose Microelectronics

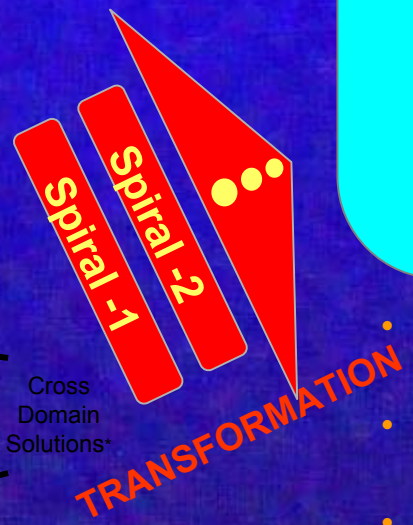
Conduct Outreach and Awareness Activities

The IA View of the GIG Architectural Transformation Is Revolutionary

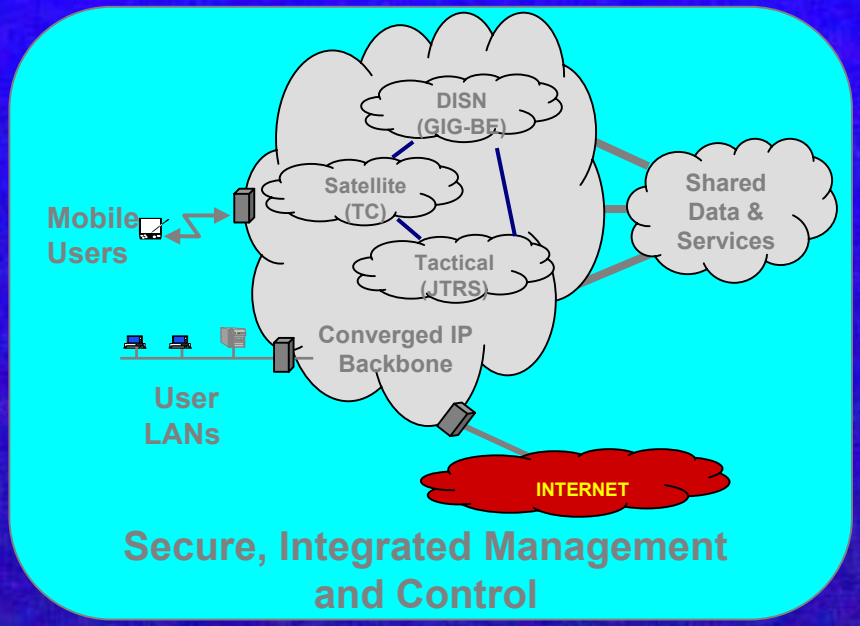
Current

- Physically isolated
- Protected information domains
- High volume cross-domain transactions
- Static system
- Boundary-to-boundary
- IA restricts user capability





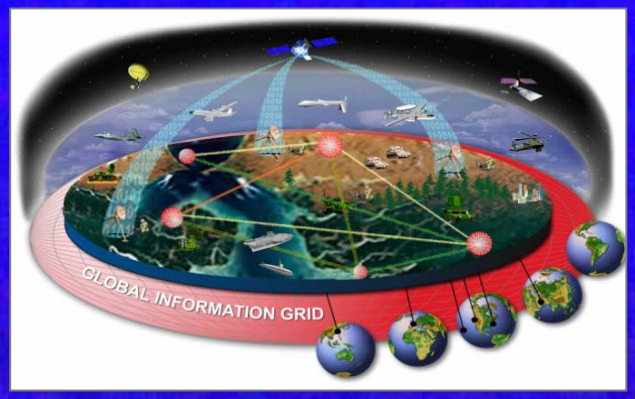
Future (implied by GIG vision)

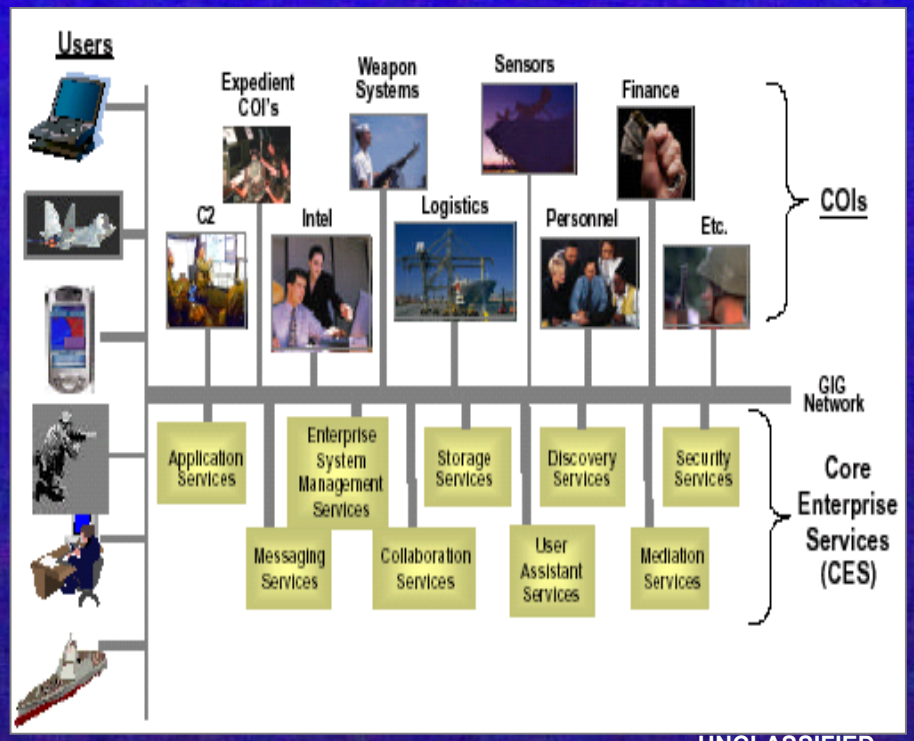


- Logical domains, based on user privileges and access controls
- Globally integrated mgt with automated collection of data
- Labeled data and registries
- Distributed access controls – identity & role-based
- User access to all required data, communications, and system resources
- Ubiquitous IA enables user capability

The Global Information Grid (GIG) Vision Implies a Fundamental Shift in Information Management, Communication, and Assurance

- Information and services accessed ubiquitously by ***authorized*** users -- both human and automated
- Fully IP-based ***highly available*** network providing:
- Seamless and ***secure end-to-end*** interconnected information environment
- Environment that recognizes who you are, and ***limits access*** based on, who and where you are
- ***Secure interoperability*** – within/ across DoD, IC and other Government, industry, international partners
- Common infrastructure support -- network management, performance monitoring, ***security management, attack sensing and response,*** etc.
- Strong focus on leveraging commercial technologies





Fundamental transformation in information management, communication, and *assurance*

COTS Strategy:

The Road to Security

Background

- Global IT Market exceeded $1 Trillion in 2003
- IA Products and Services expected to rise from $17B to over $45B in 2006
- More Application Software Development is moving Offshore
- Over 50% of the Nation's Custom Application Software Development Offshore by 2007

NSA/IAD DOES NOT HAVE RESOURCES TO BE SOLE SOURCE PROVIDER OF IA SOLUTIONS FOR OUR CUSTOMER

Today's Practice

- Partnership Agreements with Specific Vendor
  - Advantage: Can be done NOW
  - Disadvantages: Expensive, Time Consuming, and Manpower Intensive
- Partnership Agreements with Industry Leaders
  - Advantage: Access to products in development
  - Disadvantage: Long Term Commitments, Expensive, and Time Consuming
- Both Services and Products Partnership

GOAL: COTS Strategy

U.S. Commercial vendors of Information Assurance relevant information technology will provide commercial offerings (COTS) that meet the Information Assurance needs of our customers.

MUST work with our customer to better identify IA needs, so we aren't wasting time evaluating products that are not needed.

Strategy Components

- Partner with Industry
- COTS Technology
  - Use COTS to the maximum extent possible
- GOTS Slice
  - Use GOTS only when necessary
- ISSE Support
  - Help our customers select COTS products and tailor their networks
- Research Developments
  - Work with Industry to develop solutions for the future

Software Assurance

High Assurance Software

- What is it?
  - Software engineered such that its characteristics allow for it to be thoroughly analyzed and understood to determine that it does what it was designed to do and nothing more.
    - Quality
    - Trustworthiness
  - These characteristics and subsequent analysis lead to the establishment of trust.

The Threat

- Commercial Software is Being Used Everywhere
  - E-commerce Systems
  - Health Care Systems
  - Critical Infrastructure Systems
  - National Security Systems
- Foreign Influence into Commercial Software is Substantial
  - Off-shore Development
  - Foreign National Employees in the U.S.
  - Inclusion of 3rd Party Software
- Malicious Code (U.S. / Offshore)
- Insider Threat

The Threat (continued)

- Re-introduction of Code
- Visibility into Development Process Limited
- Commercial Software is Increasingly Complex
  - Windows has grown from ~6M LOC (ver 3.1) to over 30M LOC today (XP)
  - Linux base is ~3M LOC
    - Available kernel extensions and functional packages (e.g., firewall, intrusion detection, VPN) add millions more
      - » (Linux development path may follow Windows)
  - Complex Business Application Packages

The Threat (continued)

- Functionality is Rarely Removed to Support Backwards Compatibility
- Software Complexity Contributes to Instability
- Software Complexity Leads to Exploitable Errors
- Software Complexity Hinders Discovery of Malicious Code

Issues Critical to Achieving High Assurance Software

- Software Engineering Standards
- High Assurance Software Research
- Software Evaluation Procedures and Methods
- Software Development and Software Analysis Tools
- Consumer Education and Awareness

Critical Issues - Standards

- Complexity Standards (engineering)
  - Overloading Data Structures
  - Redefinition of Variables
  - Levels of Software Depth and Recursion
- Coding Standards (language specific)
  - Functions should perform only 1 task
  - Parameters should be passed by value vice reference
- Composability Standards (interfaces)
  - Interface Documentation
  - Security Policy Coordination

Critical Issues - Research

- Development Paradigms
  - Proprietary Development/Open Source
- Software Engineering Techniques
  - Modularity/Layering/Abstraction & Data Hiding
- Language Specific Issues
- Provably Secure Software
  - Formal Methods
    - Specification
    - Verification
  - Automatic Code Generation

Security-Enhanced Linux

(SELinux)

What is SELinux

- Provides flexible comprehensive mandatory access controls for Linux
- Application of NSA's Flux Advanced Security Kernel (Flask) Security Architecture
  - Builds on 12+ years of NSA's OS Security Research
- Enables security benefits of Mandatory Access Control (MAC) in Linux
  - Confines damage from malicious code
- Reference implementation being adopted by industry

Prior Research Prototypes

- SELinux latest in series of OS prototypes
  - Distributed Trusted Mach (DTMach)
  - Distributed Trusted Operating System (DTOS)
  - Flux Advanced Security Kernel (Flask)
- Each resulted in refinements to security architecture
- Built experience to deliver SELinux

Decision to move to Linux

- Recognized need to move to a mainstream platform
- Past strategies not producing desired results
- National Security Council interest in Open Source
- Technology Transfer opportunities
- Linux chosen as best alternative

NSA's Work on SELinux

- 1999 – NSA applies security architecture to Linux Kernel
  - NSA later partnered w/SCC, MITRE and NAI Labs on other aspects of the system.
- Dec 2000: NSA made initial public release of SELinux prototype
- March 2001: NSA briefed SELinux to Linux Kernel Summit
- 2001-2003: NSA partnered w/community on security framework
  - NSA re-worked SELinux to use security framework
- 2003-present: As part of COTS Strategy, worked with Industry to incorporate SELinux into commercial products (ex. Red Hat)

Commercialization

- Integration by Red Hat and other distributors
- Research on MLS
- Enhancements to management, networking, auditing, scalability
- Interest across wide variety of industries
- Planned Common Criteria Evaluation

Recognition

- Operating System Research Team – IAD Research Group – R2
  - Worked the secure Operating System for over a decade
  - Faced numerous budget cuts and still prevailed
- SELinux is a Success – continues to be excellent platform for security research
- Exposure has created many business opportunities

Remaining Challenges

- Common Criteria – more challenging in open source world
- Productization issues
- Control and Security in design of products
- Security in networked environment
- Application Architectures
- Assurance in the platform

Common Criteria

Common Criteria

- Upgrade Common Criteria – will be released Summer 2005
- International Standards
- Engage Industry and Academia

Common Criteria Recognition Arrangement (CCRA)

Certificate Producers

US
Canada
UK
Germany
France
Japan
Australia
New Zealand

Certificate Consumers

Netherlands
Finland
Greece
Italy
Norway
Spain
Israel
Sweden
Austria
Turkey
Hungary
Czech Republic

NIAP CCEVS Project Status

- As of January 2005
  - 132 products “in progress”
  - 86 certificates issued to date
  - 35 cancelled/withdrew

U.S. Approved Common Criteria Testing Laboratories

Booz, Allen & Hamilton	Linthicum, Maryland
Arca (was Cable & Wireless)	Sterling, Virginia
COACT, Inc.	Columbia, Maryland
Computer Sciences Corp.	Annapolis Junction, MD
Criterian Independent Lab	Fairmont, West Virginia
CygnaCom Solutions, Inc.	McLean, Virginia
InfoGard Laboratories, Inc	San Luis Obispo, CA
Lockheed-Martin IS&S SSO	Hanover, MD
Science Applications Int'l Corp.	Columbia, MD

….. *More Applicants Received*

Conclusion

- What is the proper assurance-model for customers using open source software?
- Is it different than proprietary software?
- I need both types!

MUST HAVE HIGH ASSURANCE

POC for NSA (IA)

Business Affairs Office (BAO)

410-854-6091

Fax: 410-854-4661

STU: 410-854-4384

Dibao@missi.ncsc.mil