

Air Force Institute of Technology

Educating the World's Best Air Force



Modeling Enterprise Security Architecture

Maj George Dalton,
Dr. John Colombi, Dr. Robert Mills

Presented by Maj George Dalton

Center for Information Security Education
& Research

U.S. AIR FORCE

28 September 2006

Integrity - Service - Excellence



Overview



- Introduction
- Security Overview
- Modeling Overview
- Problem
- Potential Solutions
- Summary

- The views expressed in this article are those of the authors and do not reflect the official policy of the United States Air Force, Department of Defense, or the United States Government.

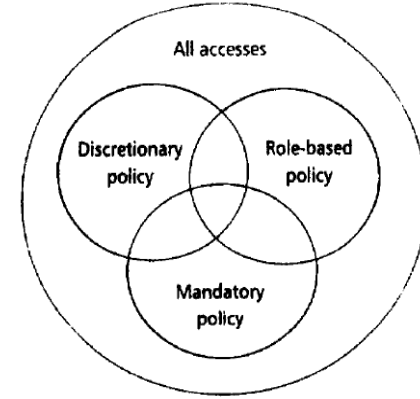


What is Security and why do we need it?

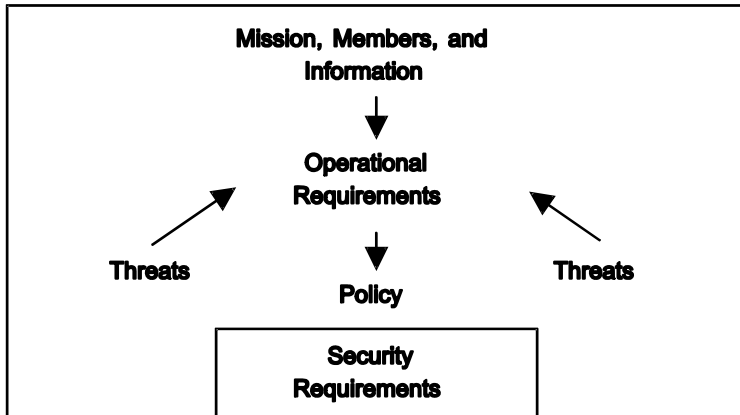


- **Confidentiality**
- **Integrity**
- **Availability**

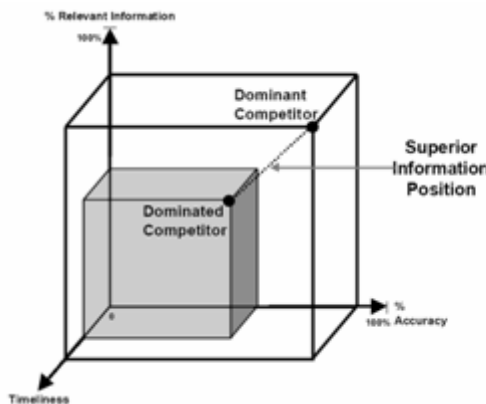
- More than just Access Control
- Risk Management
 - E-Business
 - NetCentric Operation



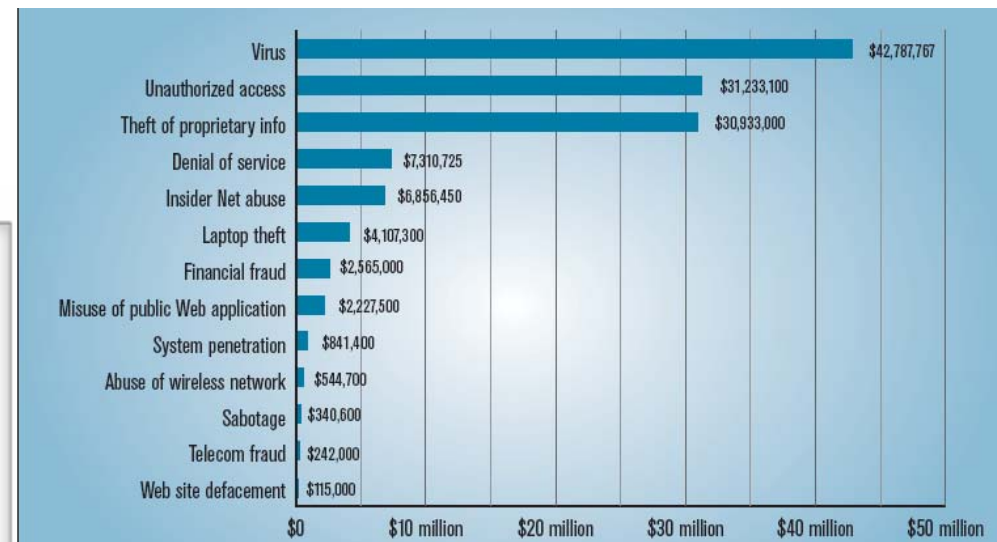
(Sandhu and Samarati, 1994)



(DoD, 1993)



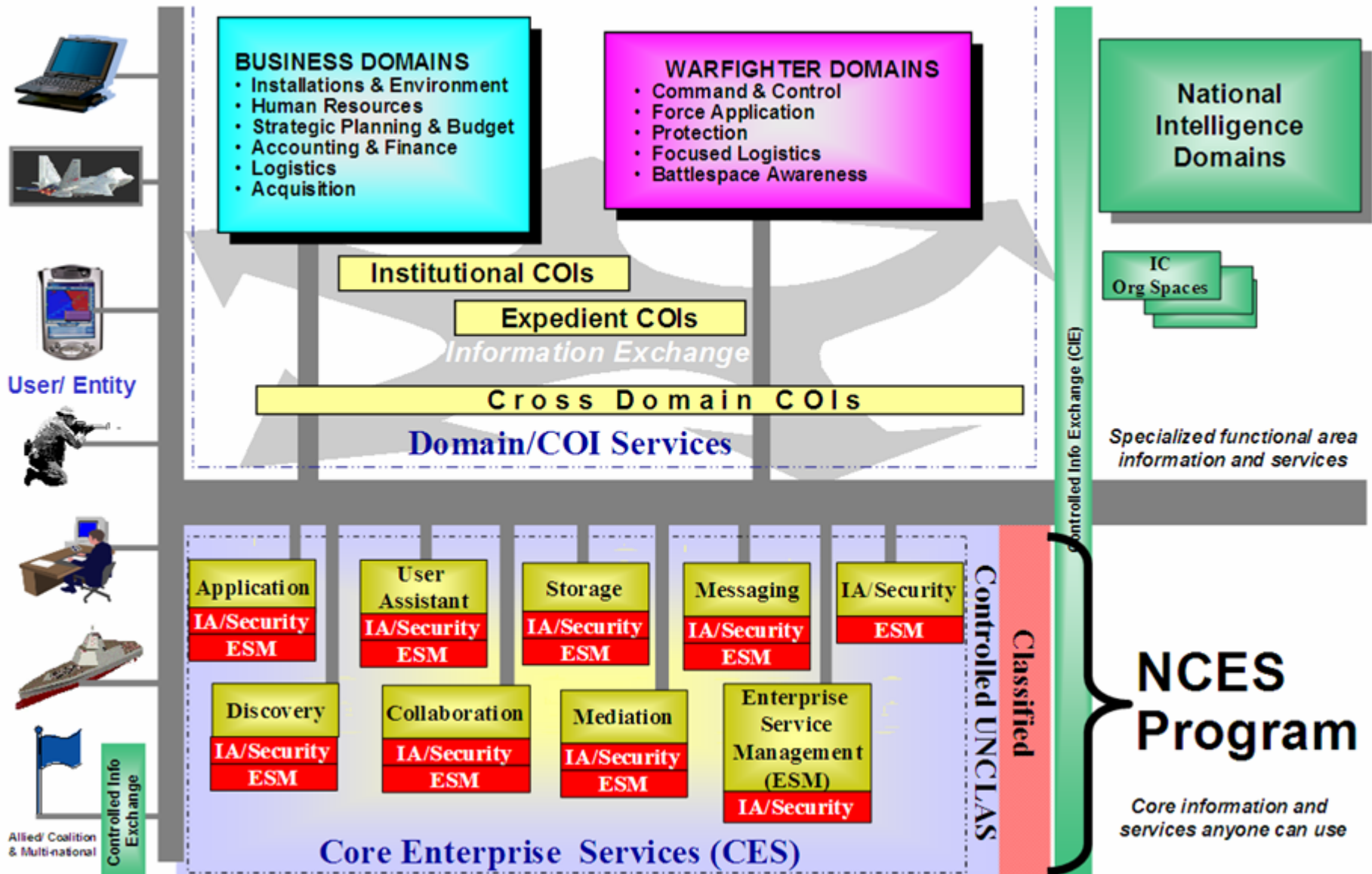
(Alberts et al., 2003, Alberts and Hayes, 2006)



2005 (Lucyshyn and Richardson., 2005)

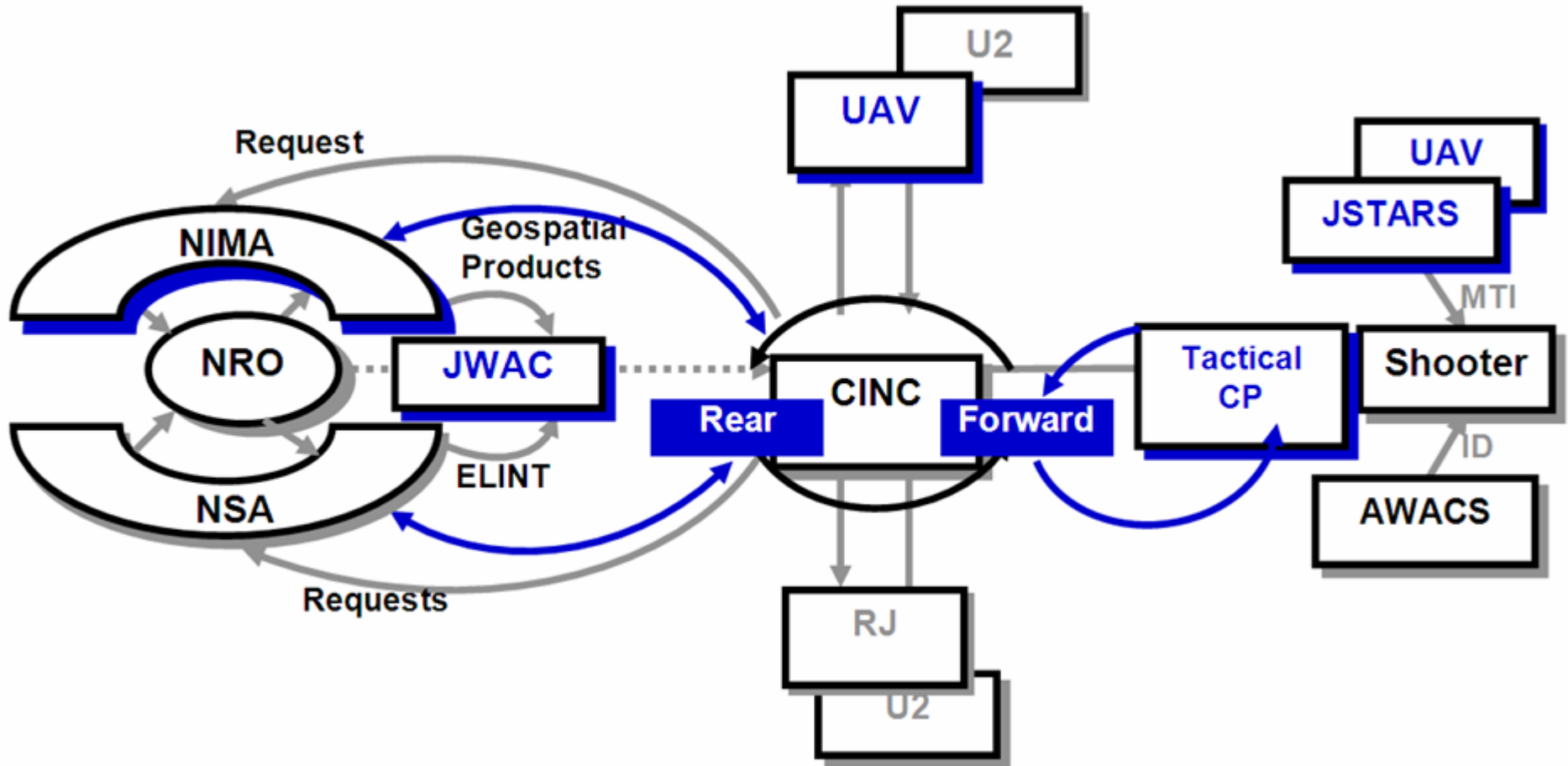


NetCentric Enterprise Services





NetCentric Warfare Example



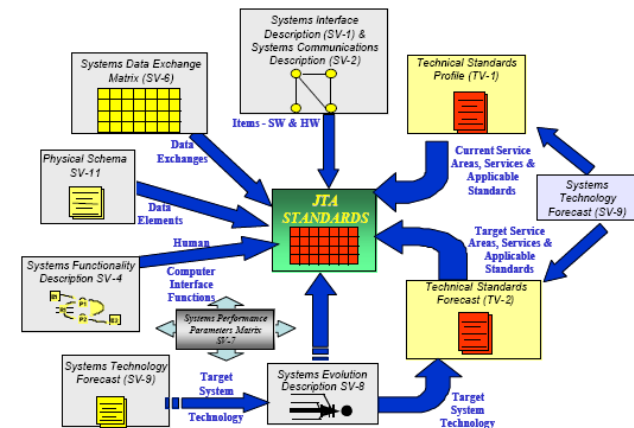
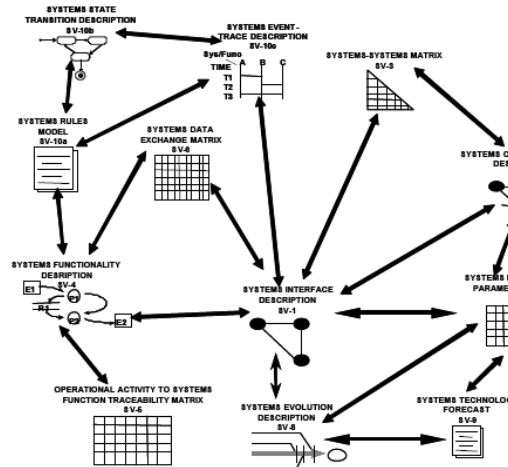
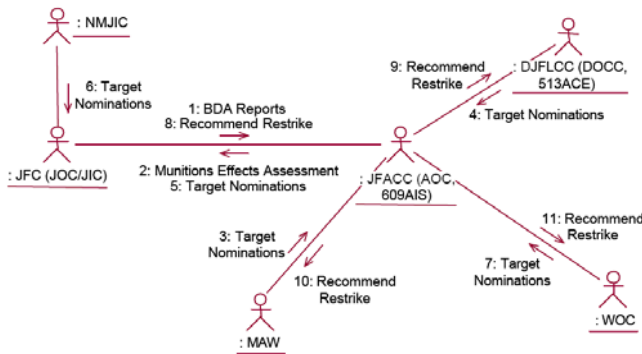
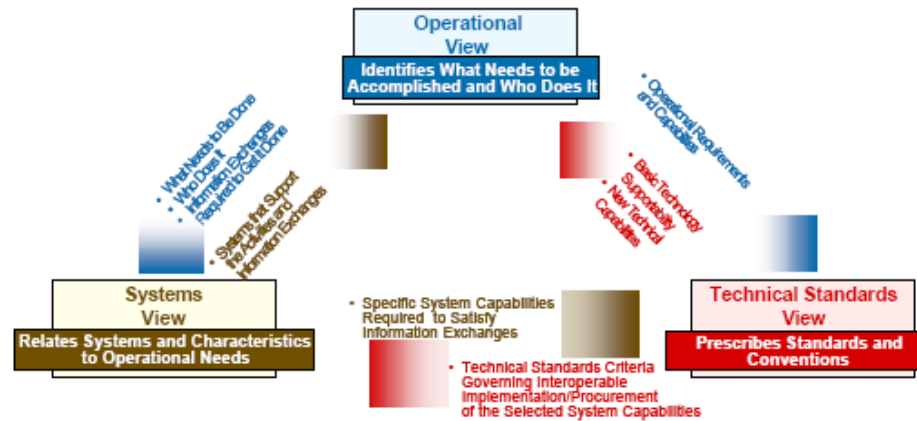
(Taylor, 2004)



DoDAF



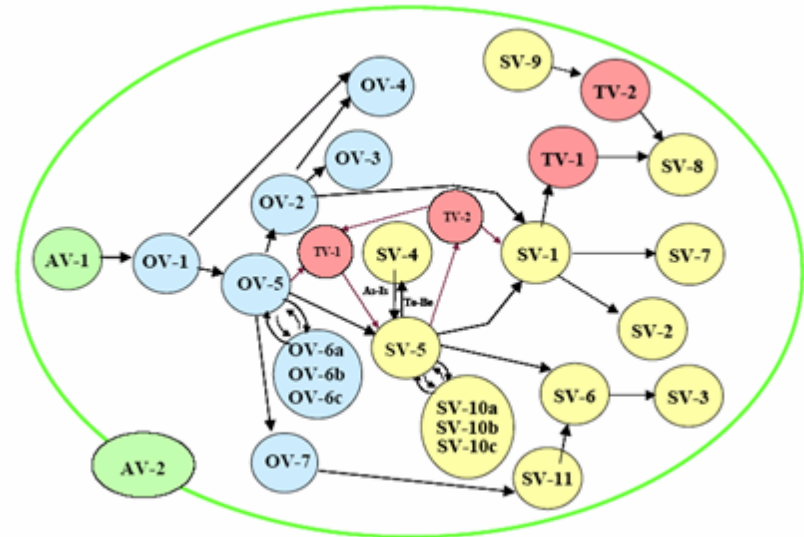
- Operational View
- System View
- Technical View



DoDAF (Continued)



Applicable View	Framework Product	Framework Product Name	General Description
All Views	AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
All Views	AV-2	Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Operational	OV-1	High-Level Operational Concept Graphic	High-level graphical/textual description of operational concept
Operational	OV-2	Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange needlines between nodes
Operational	OV-3	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
Operational	OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
Operational	OV-5	Operational Activity Model	Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
Operational	OV-6a	Operational Rules Model	One of three products used to describe operational activity—identifies business rules that constrain operation
Operational	OV-6b	Operational State Transition Description	One of three products used to describe operational activity—identifies business process responses to events
Operational	OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
Operational	OV-7	Logical Data Model	Documentation of the system data requirements and structural business process rules of the Operational View
Systems	SV-1	Systems Interface Description	Identification of systems nodes, systems, and system items and their interconnections, within and between nodes
Systems	SV-2	Systems Communications Description	Systems nodes, systems, and system items, and their related communications lay-downs
Systems	SV-3	Systems-Systems Matrix	Relationships among systems in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
Systems	SV-4	Systems Functionality Description	Functions performed by systems and the system data flows among system functions
Systems	SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to capabilities or of system functions back to operational activities
Systems	SV-6	Systems Data Exchange Matrix	Provides details of system data elements being exchanged between systems and the attributes of that exchange
Systems	SV-7	Systems Performance Parameters Matrix	Performance characteristics of Systems View elements for the appropriate time frame(s)
Systems	SV-8	Systems Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
Systems	SV-9	Systems Technology Forecast	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
Systems	SV-10a	Systems Rules Model	One of three products used to describe system functionality—identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation
Systems	SV-10b	Systems State Transition Description	One of three products used to describe system functionality—identifies responses of a system to events
Systems	SV-10c	Systems Event-Trace Description	One of three products used to describe system functionality—identifies system-specific refinements of critical sequences of events described in the Operational View
Systems	SV-11	Physical Schema	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Technical	TV-1	Technical Standards Profile	Listing of standards that apply to Systems View elements in a given architecture
Technical	TV-2	Technical Standards Forecast	Description of emerging standards and potential impact on current Systems View elements, within a set of time frames





Zachman



Planner View








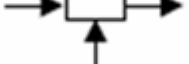
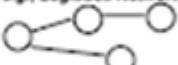
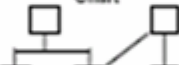
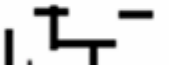


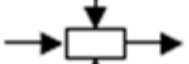
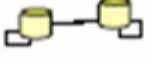

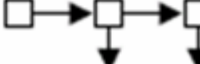

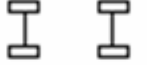
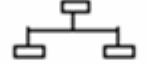
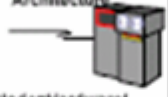

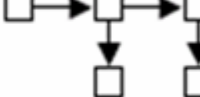







Owner View

Designer View

Builder View

Subcontractor View

Functioning Enterprise

	Data	Function	Network	People	Time	Motivation
	List of Things Important to Business  Entity=Class of Business Thing	List of Processes the Business Performs  Function=Class of Business Process	List of Locations Important to Business  Node=Major Business Location	List of Organizations Important to Business  Agent=Major Org Unit	List of Events Significant to Business  Time=Major Business Event	List of Business Goals/Strategies  End/Means=Major Business Goal/CSF
	e.g., Entity Relationship Diagram  Ent=Business Entity Rel=Business Rule	e.g., Function Flow Diagram  Function=Business Process	e.g., Logistics Network  Node=Business Location Link=Business Linkage	e.g., Organization Chart  Agent=Org Unit Work=Work Product	e.g., Master Schedule  Time=Business Event Cycle=Business Cycle	e.g., Business Plan  End=Business Objectives Means=Business Strategy
	e.g., Data Model  Entity=Data Entity Relationship=Data Relationship	e.g., Data Flow Diagram  Funct=Appl Function Arg=User Views	e.g., Distributed System Architecture  Node=Info Sys Funct Link=Line Char	e.g., Human Interface Architecture  Agent=Role Work=Deliverable	e.g., Processing Structure  Time=System Event Cycle=Processing Cycle	e.g., Knowledge Architecture  End=Criterion Means=Option
	e.g., Data Design  Entity=Segment/Row Relationship=Pointer/Key	e.g., Structure Chart  Funct=Computer Funct Arg=Screen/Device/Formats	e.g., System Architecture  Node=Hardware/System Software Link=Line Specification	e.g., Human/Technology Interface  Agent=User Work=Job	e.g., Control Structure  Time=Execute Cycle Cycle=Component Cycle	e.g., Knowledge Design  End=Condition Means=Action
	e.g., Data Definition Description  Ent=Fields Rel=Addresses	e.g., Program  Funct=Language Strnts Arg=Control Blocks	e.g., Network Architecture  Node=Addresses Link=Protocols	e.g., Security Architecture  Agent=Identity Work=Transaction	e.g., Timing Definition  Time=Interrupt Cycle Cycle=Machine Cycle	e.g., Knowledge Definition  End=Subcondition Means=Step



Others



- Java 2 Enterprise Edition (J2EE)
- Microsoft .NET
- International Standards Organization Open Distributed Processing (ISO ODP)
- The Open Group Architecture Framework (TOGAF)



Security Architecture

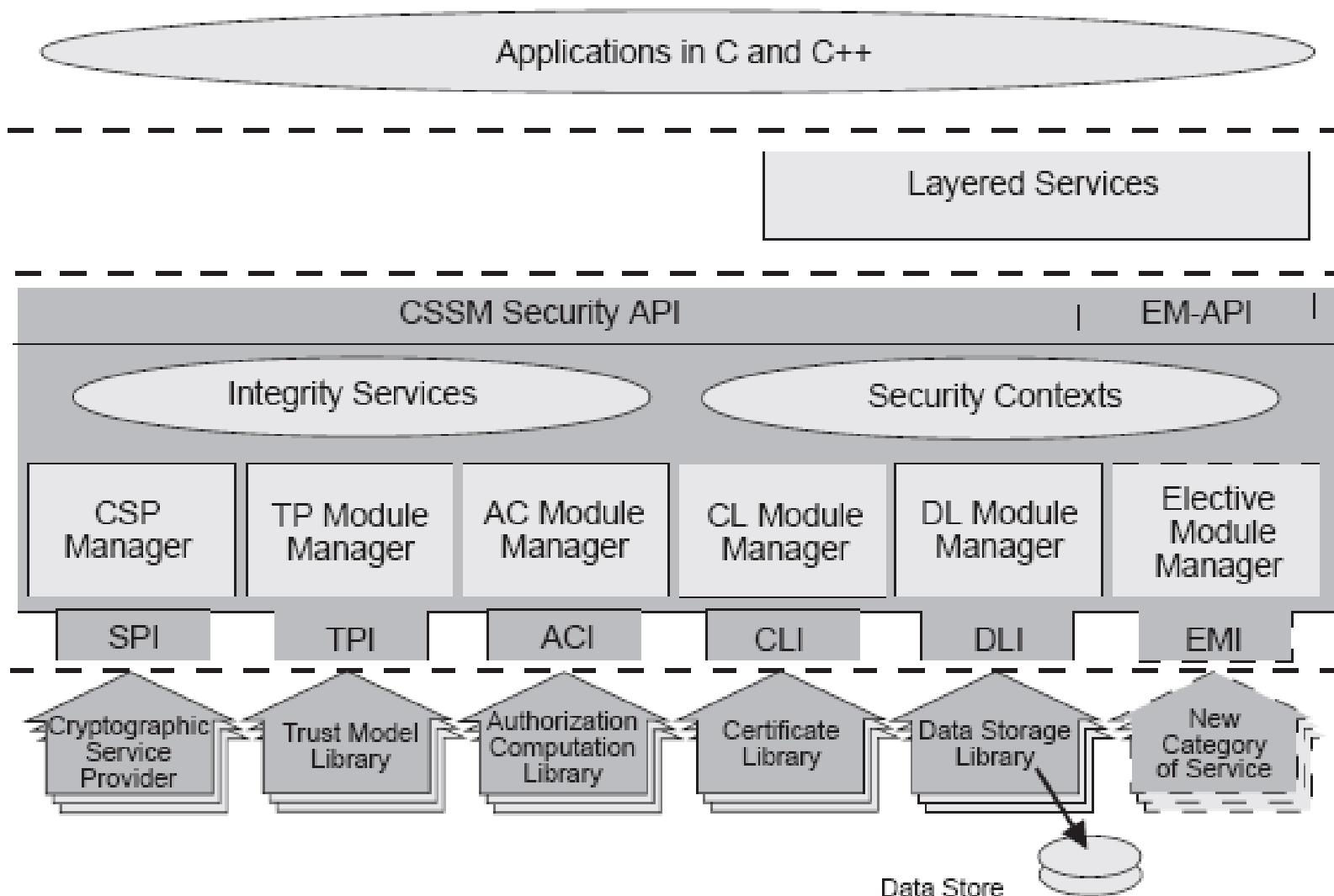


- What is a Security Architecture?
- Is it separate from a Systems Architecture?
- Examples of Security Architectures
 - DoD Goal Security Architecture (DGSA)
 - Open Management Group (OMG) Common Data Security Architecture
 - Network Centric Operations and Warfare (NCOW) reference Model

These Architectures and Models Don't provide an assessment of current security



Example of Security Architecture



Can a Decision Maker use this to determine where to expend resources?

(CDSA) (2000)



Other Modeling Tools



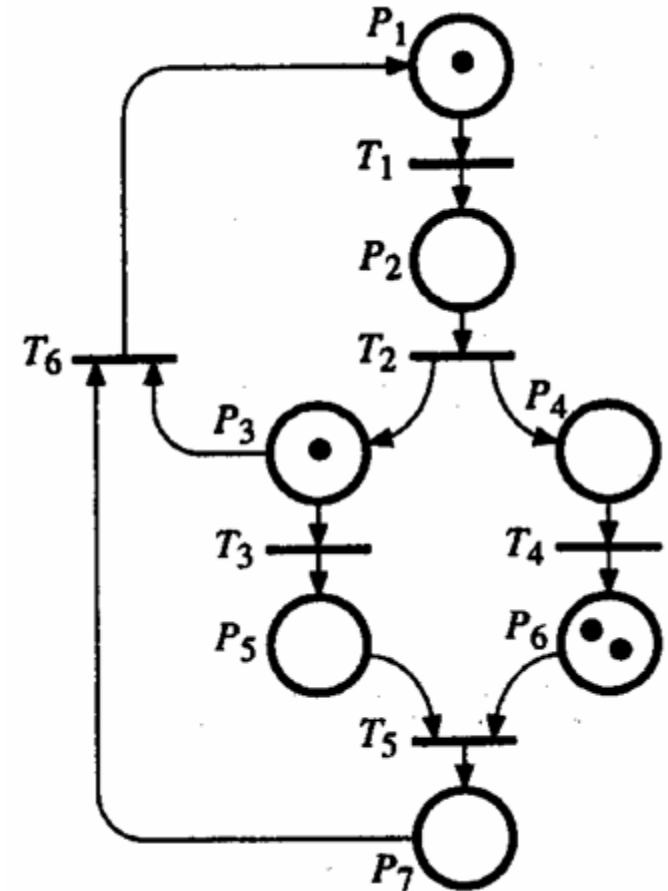
- Petri Nets
- Attack Trees
- Many others...



Petri Nets



- Places, Transitions, Arcs, and Tokens
- Described by 4-tuple
 - PN (P,T,I,O) where:
 - P is the set of places, T is the set of transitions, I and O are the set of input and output arcs



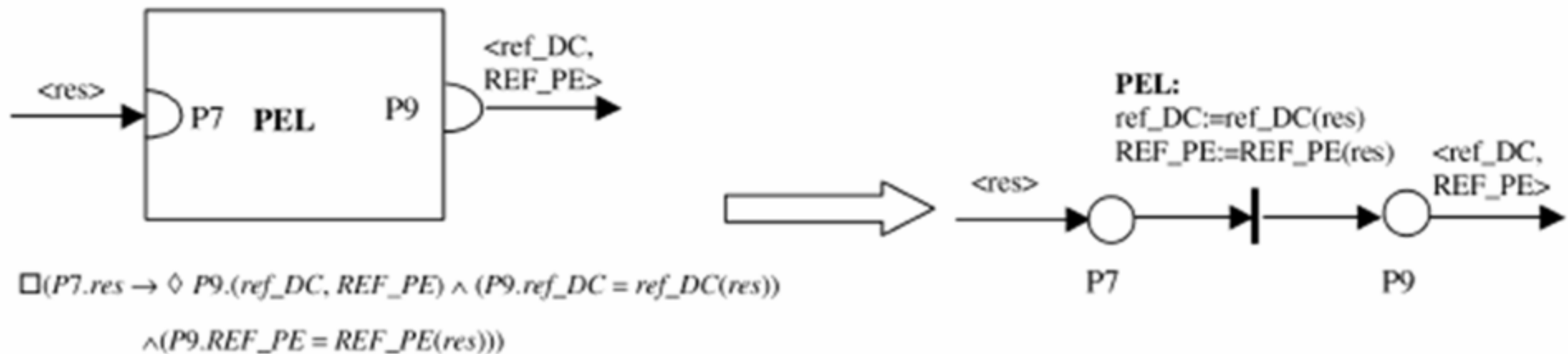
(David and Alla, 2005)



Using PNs to Model Security



- Can be used to Hierarchically Model System Activities
 - PNs can be used to model stochastic processes
 - Colored PNs enable modeling of system data flows using types
- Easy to Generate and Simulate
- Can be used to create Executable Architectures

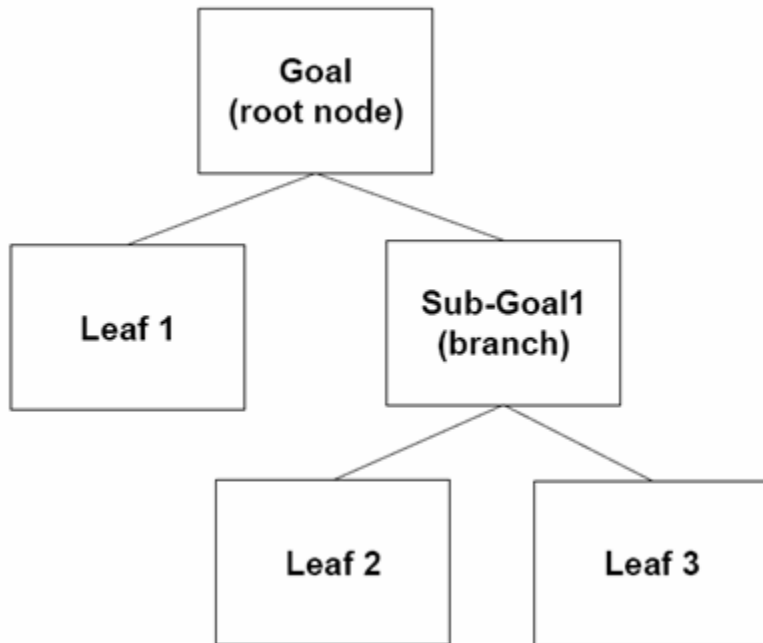




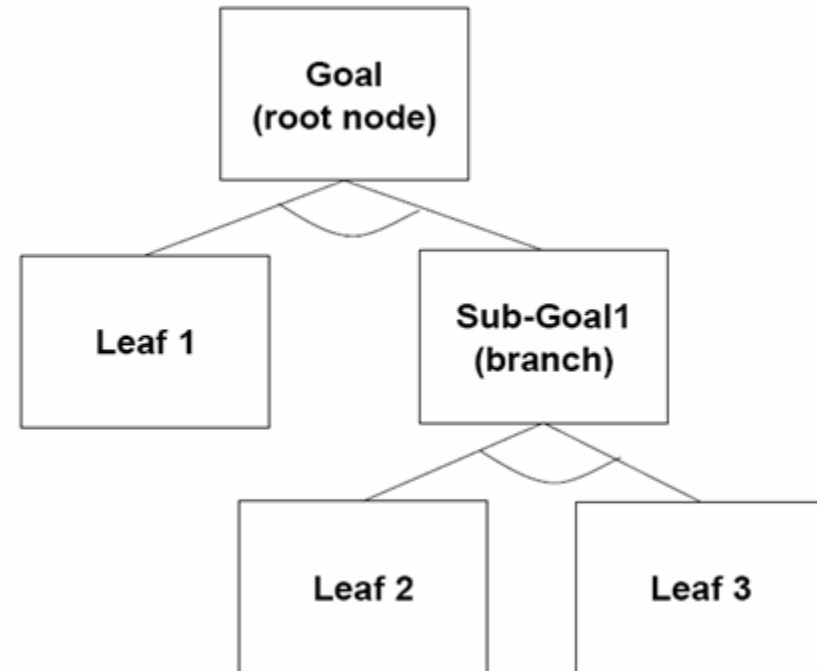
Attack Trees



- 1. Goal
 - 1.1. Leaf 1 (OR)
 - 1.2. Sub-Goal 1
 - 1.2.1. Leaf 2 (OR)
 - 1.2.2. Leaf 3



- 2. Goal
 - 2.1. Leaf 1 (AND)
 - 2.2. Sub-Goal 1
 - 2.2.1. Leaf 2 (AND)
 - 2.2.2. Leaf 3

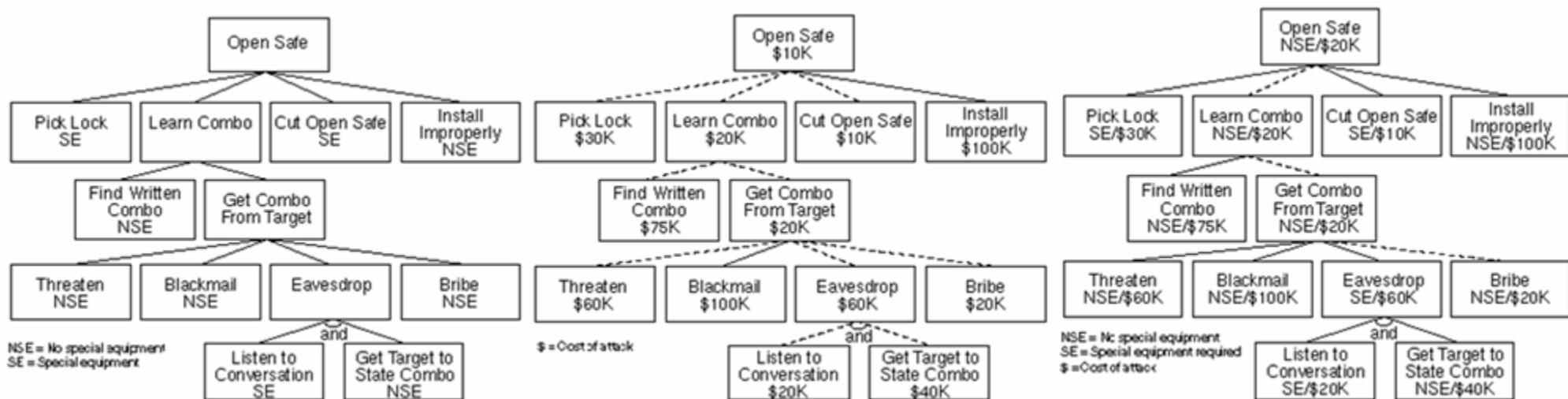




Using Attack Trees to Model Security

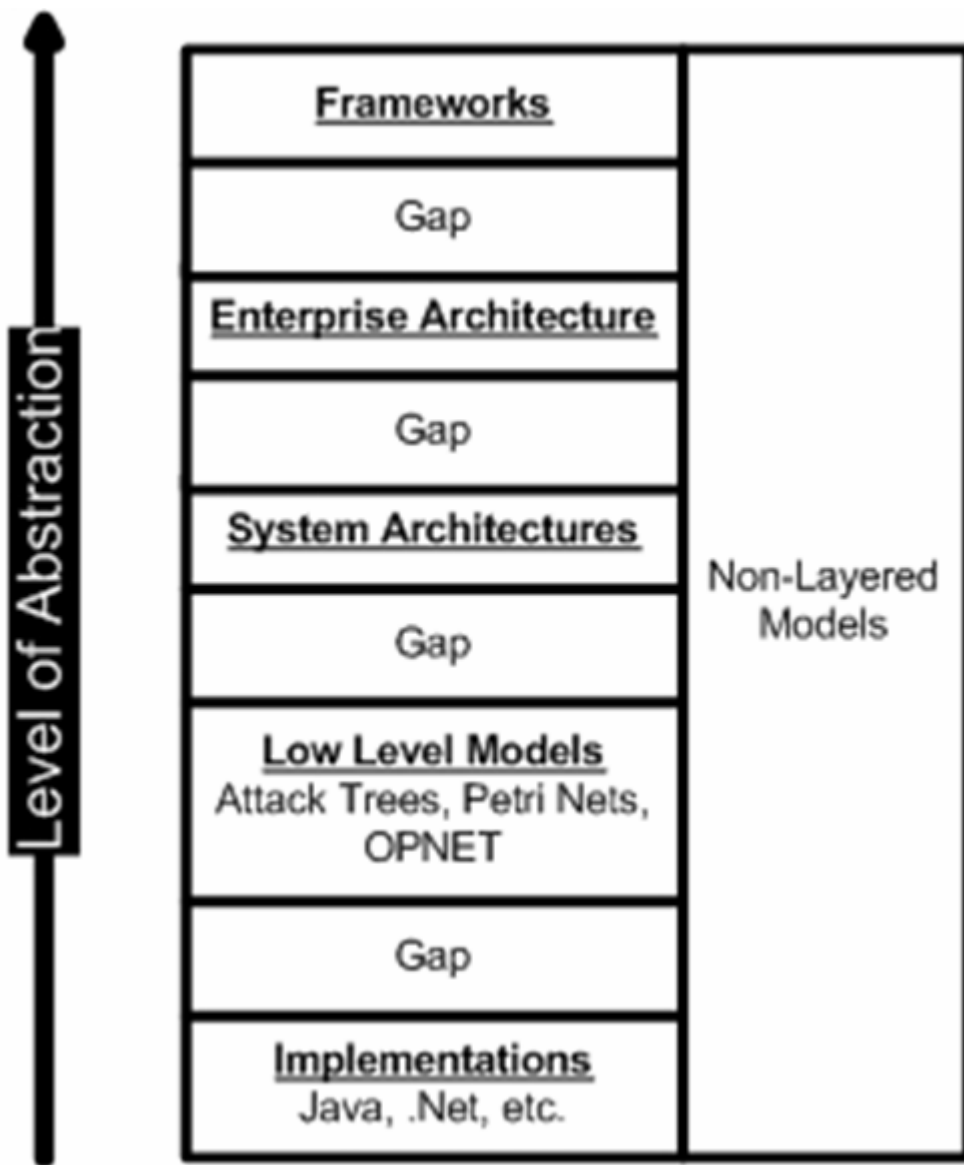


- Allow Threat Modeling
- Can assign values to Leaves
- Values can be rolled up to develop optimal response or most appropriate Course of Action
- Decision Maker can then choose where to invest limited resources





Hierarchy of Models





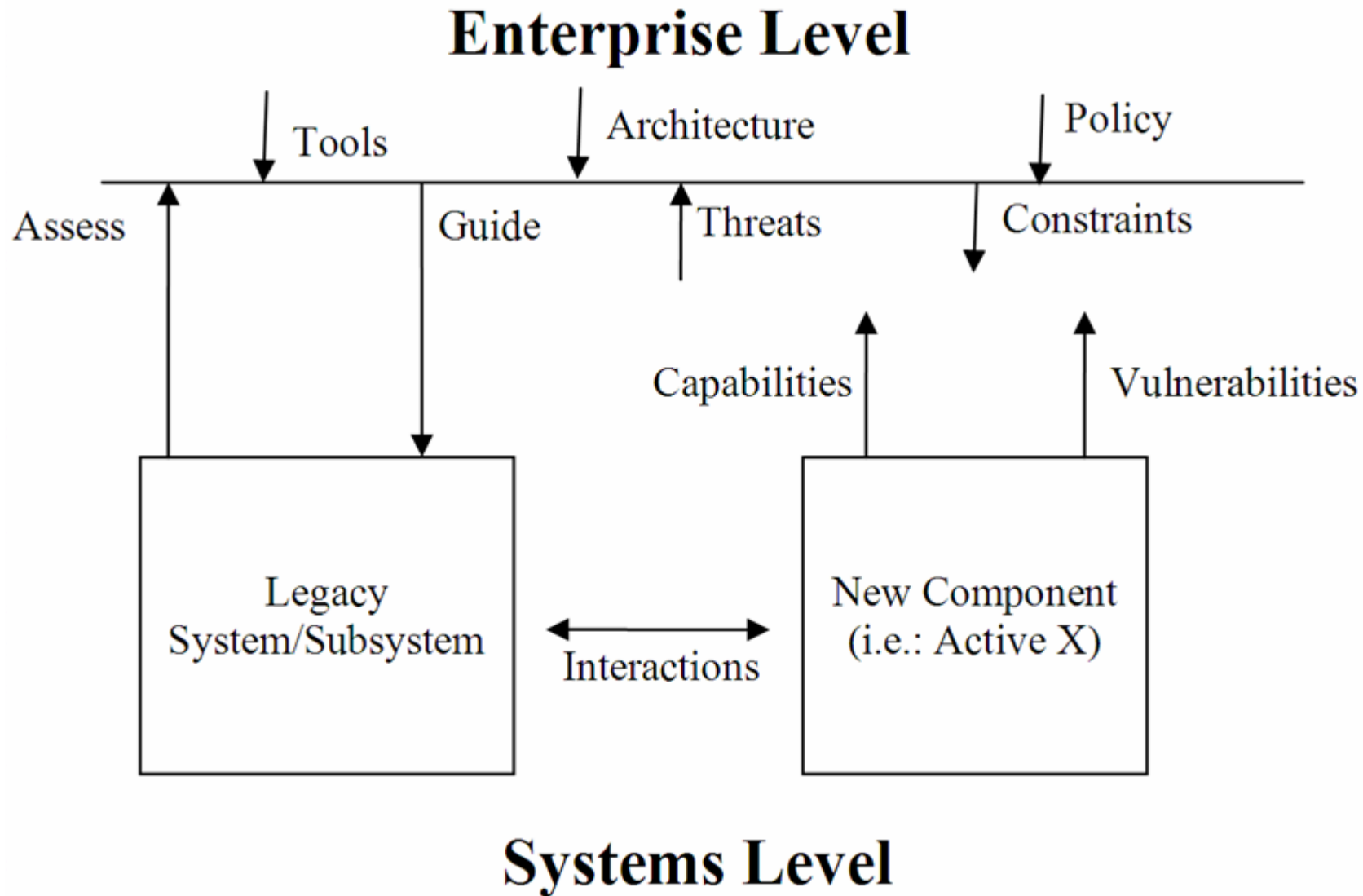
Problem



- Combatant Commanders and Chief Information Officers are not able to immediately determine mission effects of enterprise component outages or system-wide attacks
- No Courses of Action (COAs) with cost benefit analysis available to them
- Speed of the internet may prohibit effective human interdiction
- Enterprise to Enterprise security at risk without a global integrated security architecture



Security Aspects of Adding New Components to the Enterprise





Potential Solutions



- Technology
 - Enterprise Architectures based on Common/Standard Frameworks with integrated Security Architecture
 - Must be Adaptive and Proactive
 - Must be able to Respond to Failures and Attacks and Learn from them
 - Make architectures executable by using a hierarchy of models
- Policies
 - Standardize Policies
 - “Tailorable” to Individual Enterprises
- Procedures
 - Common Procedures built on Sound Security Principle
 - Develop Courses of Action that support Policies and Take Advantage of Technology
 - Automate Response when Appropriate



Summary



- Introduction
- Security Overview
- Modeling Overview
- Problem
- Potential Solutions
- Summary

- The views expressed in this article are those of the authors and do not reflect the official policy of the United States Air Force, Department of Defense, or the United States Government.



References



- [1] "Merriam-Webster Online Dictionary," Merriam-Webster
- [2] USAF, "Air Force Doctrine Document 1 (AFDD1) Air Force Basic Doctrine," 2003.
- [3] USAF, "Air Force Doctrine Document 2-5 (AFDD2-5) Information Operations," 2005.
- [4] T. Erl, *Service-Oriented Architecture: Concepts, Technology, and Design*: Prentice Hall, 2005.
- [5] IDA, "Security Activity Budget Estimates ": Institute for Defense Analyses, 2004.
- [6] W. Lucyshyn and R. Richardson., "2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY," Computer Security Institute, 2005.
- [7] L. G. H. D. Raduege, "Transforming the GIG," presented at SPACECOM, Colorado Springs, CO, 2004.
- [8] D. S. Alberts, J. J. Garstka, and F. P. Stein, *NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority*, 5th Edition (Revised) ed: C4ISR Cooperative Research Program (CCRP), 2003.
- [9] D. S. Alberts and R. E. Hayes, *UNDERSTANDING COMMAND AND CONTROL*. Washington, D.C.: DoD Command and Control Research Program, 2006.
- [10] E. G. Taylor, "Transformation to Net-Centric Ops," presented at SPACECOM, 2004.
- [11] J. A. Zachman, "Framework for Enterprise Architecture."
- [12] DoD, "DoD Architecture Framework (DoDAF) Version 1.0 ", vol. I, 2004
- [13] DoD, "Department of Defense (DoD) Goal Security Architecture (DGSA) Version 1.0," Defense Information Systems Security Program, 1993.
- [14] "Technical Standard, Common Security: CDSA and CSSM, Version 2.3," The Open Group, 2000.
- [15] E. H. Sibley, J. B. Michael, and R. S. Sandhu, "A case-study of security policy for manual and automated systems," 1991.
- [16] Y. Deng, J. Wang, J. J. P. Tsai, and K. Beznosov, "An approach for modeling and analysis of security system architectures," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, pp. 1099-1119, 2003.
- [17] T. K. Thomas and R. S. Sandhu, "A Trusted Subject Architecture for Multilevel Secure object-Oriented Databases," *IEEE Transactions of Knowledge and Data Engineering*, vol. Vol 8, 1996.
- [18] K. Jensen, "A brief introduction to colored Petri nets.," presented at Proc. Workshop on the Applicability of Formal Models, Aarhus, Denmark, 1998.
- [19] K. Jensen, "An Introduction to the Practical Use of Coloured Petri Nets," *In: W. Reisig and G. Rozenberg (eds.): Lectures on Petri Nets II: Applications, Lecture Notes in Computer Science*, vol. vol. 1492, pp. 237-292, 1998.
- [20] L. M. Kristensen, S. Christensen, and K. Jensen, "The practitioner's guide to coloured Petri nets," *International Journal on Software Tools for Technology Transfer*, vol. 2, pp. 98-132, 1998.



References



- [21] S.-Y. Lim, J.-H. Ko, E.-A. Jun, and G.-S. Lee, "Specification and analysis of n-way key recovery system by Extended Cryptographic Timed Petri Net," *Journal of Systems and Software*, vol. 58, pp. 93-106, 2001.
- [22] M. Gao and M. Zhou, "Fuzzy intrusion detection based on fuzzy reasoning Petri nets," presented at Systems, Man and Cybernetics, 2003. IEEE International Conference on 2003.
- [23] R. Bouroulet, H. Klaudel, E. Pelz, M. Kishinevsky, P. Darondeau, M. Kishinevsky, and P. Darondeau, "A semantics of Security Protocol Language (SPL) using a class of composable high-level Petri nets," presented at Proceedings. Fourth International Conference on Application of Concurrency to System Design, Los Alamitos, CA, 2004.
- [24] J. Joshi and A. Ghafoor, "A Petri-net based multilevel security specification model for multimedia documents," presented at IEEE International Conference on Multi-Media and Expo, 2000.
- [25] K. Minami and D. Kotz, "Secure Context-Sensitive Authorization," presented at Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on 2005.
- [26] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *Communications Magazine, IEEE*, vol. 32, pp. 40-48, 1994.
- [27] M. G. Fugini and G. Martella, "A Petri-net model of access control mechanisms," *Information Systems*, vol. 13, pp. 53-63, 1988.
- [28] D. E. Bell and L. J. LaPadula, "Secure computer system: Unified exposition and Multics interpretation," The MITRE Corporation, 1976.
- [29] K. Juszczyszyn, "Verifying enterprise's mandatory access control policies with coloured Petri nets," presented at Proceedings of the Twelfth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises., 2003.
- [30] Y. Jiang, L. Chuang, C. Zhen, Y. Hao, A. M. Memon, and A. M. Memon, "Using Petri nets to verify access policies in mandatory access control model," presented at Proceedings of the 2004 IEEE Conference on Information Reuse and Integration Piscataway, NJ, 2004.
- [31] M.-K. Lee, H. R. Arabnia, and Y. Mun, "Stability verification of proxy firewall using coloured Petri nets," presented at International Conference on Security and Management, Athens, GA, 2003.
- [32] P. Stephenson, "Modeling of Post-Incident Root Cause Analysis," *International Journal of Digital Evidence*, vol. 2, 2003.
- [33] P. Stephenson, "The application of Formal Methods to Root Cause Analysis of Digital Incidents," *International Journal of Digital Evidence*, vol. 3, 2004.
- [34] P. Stephenson, "Expanding on the use of Colored Petri Nets," *Computer Fraud & Security*, pp. 17-20, 2004.
- [35] B. Schneier, "Secrets & Lies: Digital Security in a Networked World." New York: John Wiley & Sons, 2000.
- [36] M. S. Pallos, "Attack Trees: It's a Jungle Out There – Seeing Your System through a Hacker's Eyes," *WebSphere Online Journal*, vol. 3, 2004.
- [37] B. Schneier, "Modeling Security Threats," in *Dr. Dobbs Journal*, 1999.
- [38] (IWG), I. W. G. O. C. S. A. I. A. (2006) Federal Plan for Cyber Security and Information Assurance Research and Development. IN COUNCIL, N. S. A. T. (Ed.), NCO/NITRD National Coordination Office for Networking and Information Technology Research and Development.

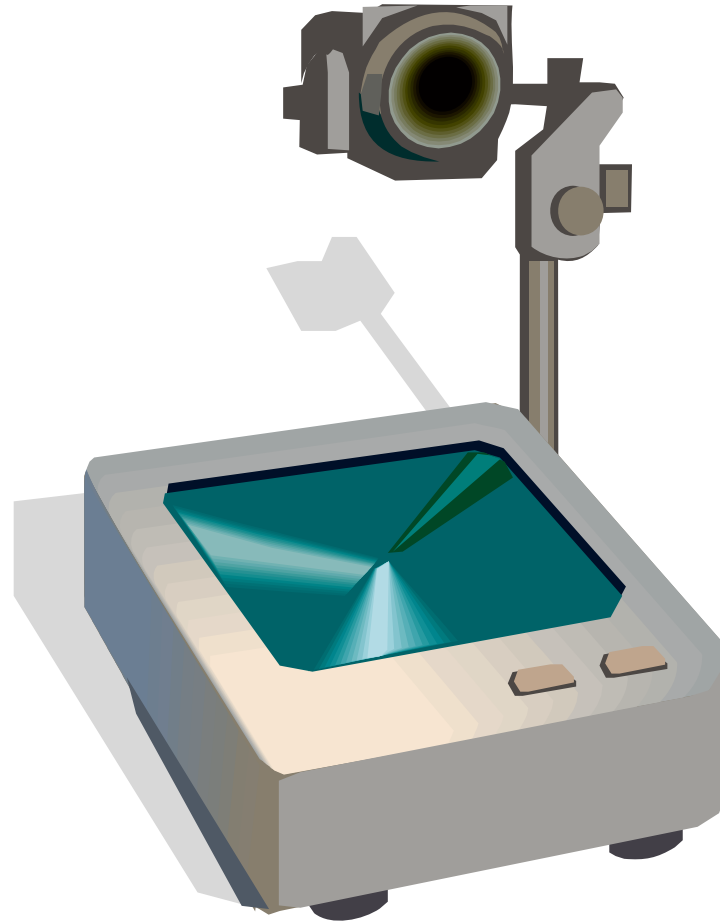


Questions





Backup Slides





Key R&D Areas



- Functional Cyber Security
 - Authentication, Authorization, and Trust Management
 - Access Control and Privilege Management
 - Attack Protection, Prevention, and Preemption
 - Large-Scale Cyber Situational Awareness
 - Automated Attack Detection, Warning, and Response
 - Insider Threat Detection and Mitigation
 - Detection of Hidden Information and Covert Information Flows
 - Recovery and Reconstitution
 - Forensics, Traceback, and Attribution
- Securing the Infrastructure
 - Secure Domain Name System
 - Securing Routing Protocols
 - IPv6, OPsec, and Other Internet Protocols
 - Secure Process Control Systems
- Domain-Specific Security
 - Wireless Security
 - Secure Radio Frequency Identification
 - Security of Converged Networks and Heterogeneous Traffic
 - Next-Generation Priority Services
- Cyber Security and Information Assurance Characterization and Assessment
 - Software Quality Assessment and Fault Characterization
 - Detection of Vulnerabilities and Malicious Code
 - Cyber Security Standards
 - Metrics Software Testing and Assessment Tools
 - Risk-Based Decision Making
 - Critical Infrastructure Dependencies and Interdependencies



Key R&D Areas (Cont)



- Foundations for Cyber Security and Information
 - Hardware and Firmware
 - Secure Operating Systems
 - Security-Centric Programming Languages
 - Security Technology and Policy Management Methods
 - and Policy Specification Languages
 - Information Provenance
 - Information Integrity
 - Cryptography
 - Multi-Level Security
 - Secure Software Engineering
 - Fault-Tolerant and Resilient Systems
 - Integrated, Enterprise-Wide Security Monitoring and Management
 - Analytical Techniques for Security Across the IT Systems Engineering Life Cycle
- Enabling Technologies for Cyber Security and Information Assurance R&D
 - Cyber Security and Information Assurance R&D Testbeds
 - IT System Modeling, Simulation, and Visualization
 - Internet Modeling, Simulation, and Visualization
 - Network Mapping
 - Red Teaming
- Advanced and Next-Generation Systems and Architectures
 - Trusted Computing Base Architectures
 - Inherently Secure, High-Assurance, and Provably Secure Systems and Architectures
 - Composable and Scalable Secure Systems
 - Autonomic Systems
 - Architectures for Next-Generation Internet Infrastructure
 - Quantum Cryptography
- Social Dimensions of Cyber Security and Information Assurance
 - Trust in the Internet
 - Privacy