Tools to Support Enterprise Assurance Arguments

Judith N. Froscher
Center for High Assurance Computer Systems
Naval Research Laboratory

March 30, 2001

Froscher@itd.nrl.navy.mil

Background

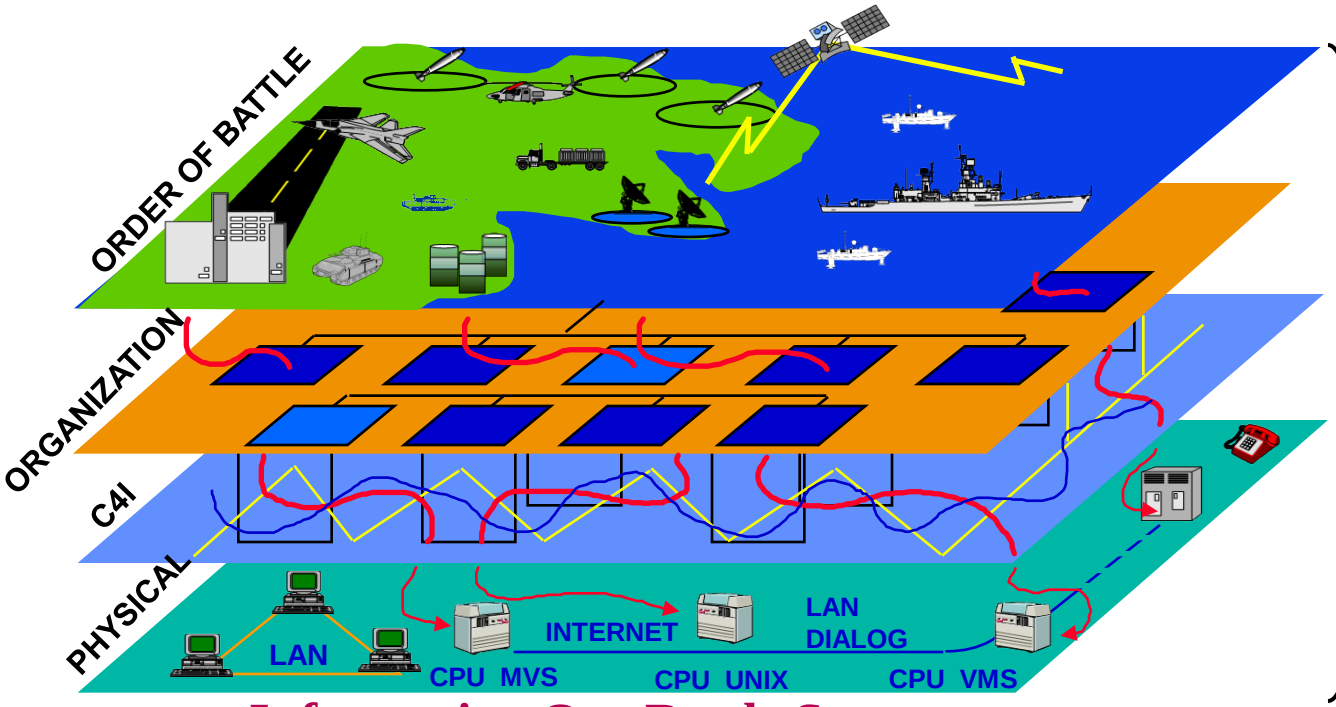
- Today, IT plays a principal role
  - Security of information systems directly or indirectly affects organizations (industry, government, military, and even citizenry)
- IA problems become more important
  - Especially, for system of systems
  - When components depend on each other

Problems

- For a trusted system
  - Designers and assessors must clearly understand
    - Causality, relationships, vulnerability, threats, system-level viewpoints, and enterprise objectives
  - Decision makers must make informed decisions based on understandable risk
- To achieve this,
  - Related assurance arguments are derived and described efficiently in an understandable way
    - Vulnerabilities are explicitly identified with clear indication of relationship to overall system security posture

Network-centric Warfare Demands a SECURE, SURVIVABLE Information Grid

PROTECT, DETECT, RESPOND, RECOVER, SURVIVE

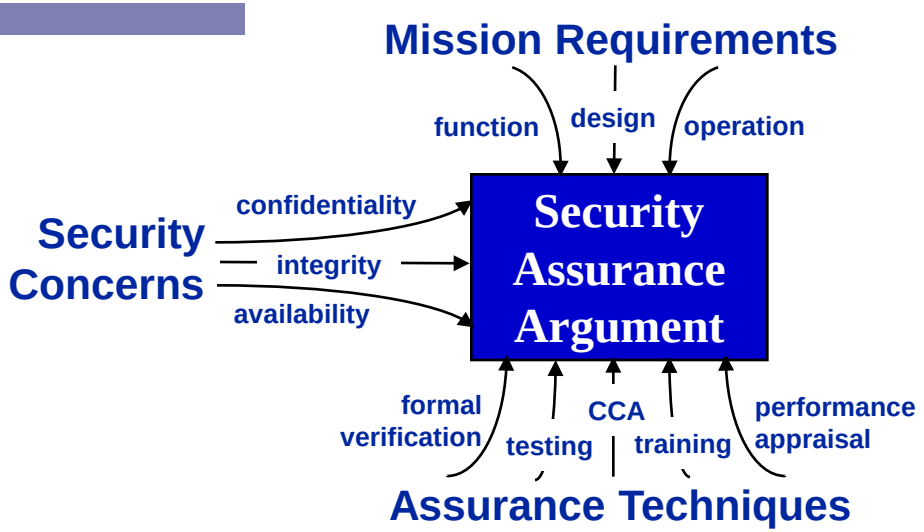


THREATS

- Nation-states
- Insiders
- Terrorist Org.
- Ankle-biters
- User mistakes
- Easter eggs

Information Ops Battle Space

What Is Needed?



- Need tools to construct comprehensive/convincing assurance argument for the enterprise
- Most existing support focuses on
  - limited part of problem (e.g., confidentiality)
  - particular assurance techniques (e.g., formal verification)
- Little technology exists for combining assurance evidence into coherent, compelling whole

Contributing Methods

- **Enterprise Certification Methodology (ECM) (NRL)**
  - **method for partitioning requirements into primary security disciplines and expressing them as assertions and assumptions**
  - **focuses on finding vulnerabilities due to invalid assumptions**
- **Goal Structured Notation (York University)**
  - **graphical notation developed for elaborating safety arguments**
  - **focuses on developing an overview of the assurance argument**
- **Methodically Organized Argument Trees (Kienzle)**
  - **method for refining assurance arguments in a balanced way**
  - **focuses on decomposing security goals as the conjunction/disjunction of sub-goals**
- **Network Rating Methodology (NSA)**
  - **method for evaluating the total security of any network**
  - **focuses on defining the assurance needs and describing how and why a system satisfies these needs in a structured way**

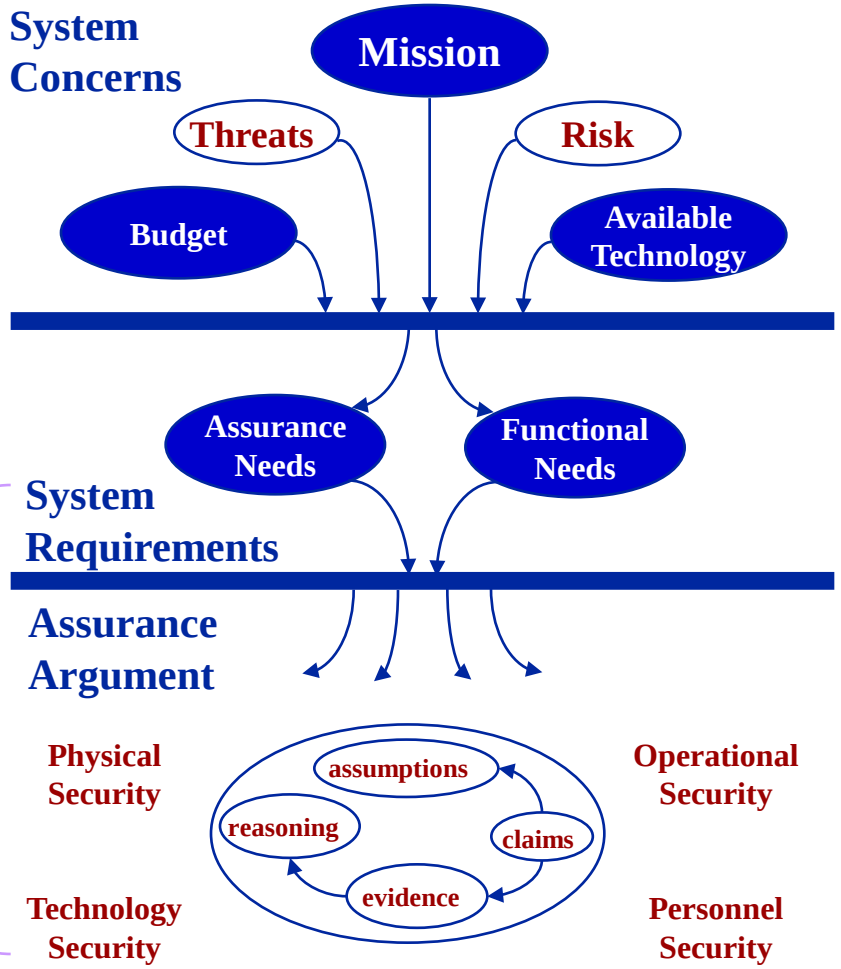
Tool Development: Teaming Up With NSA

NSA

Elicitor-level Analysis

NRM-level Analysis

NRL



Assurance Argument Map

- The assurance map is the representation of the assurance strategy
- We have introduced the concept of an assurance argument map
  - To depict the claim trees of causality, relationships, vulnerability, threats, system-level viewpoints, and enterprise objectives for target systems

Approach

- We have developed
  - A methodology (ECM)
    - To derive and organize the related assurance arguments effectively
  - A Language (CAML)
    - To describe a map of assurance arguments
  - Tools (VNRM, SANE)
    - To help users develop the assurance argument maps in CAML based on ECM

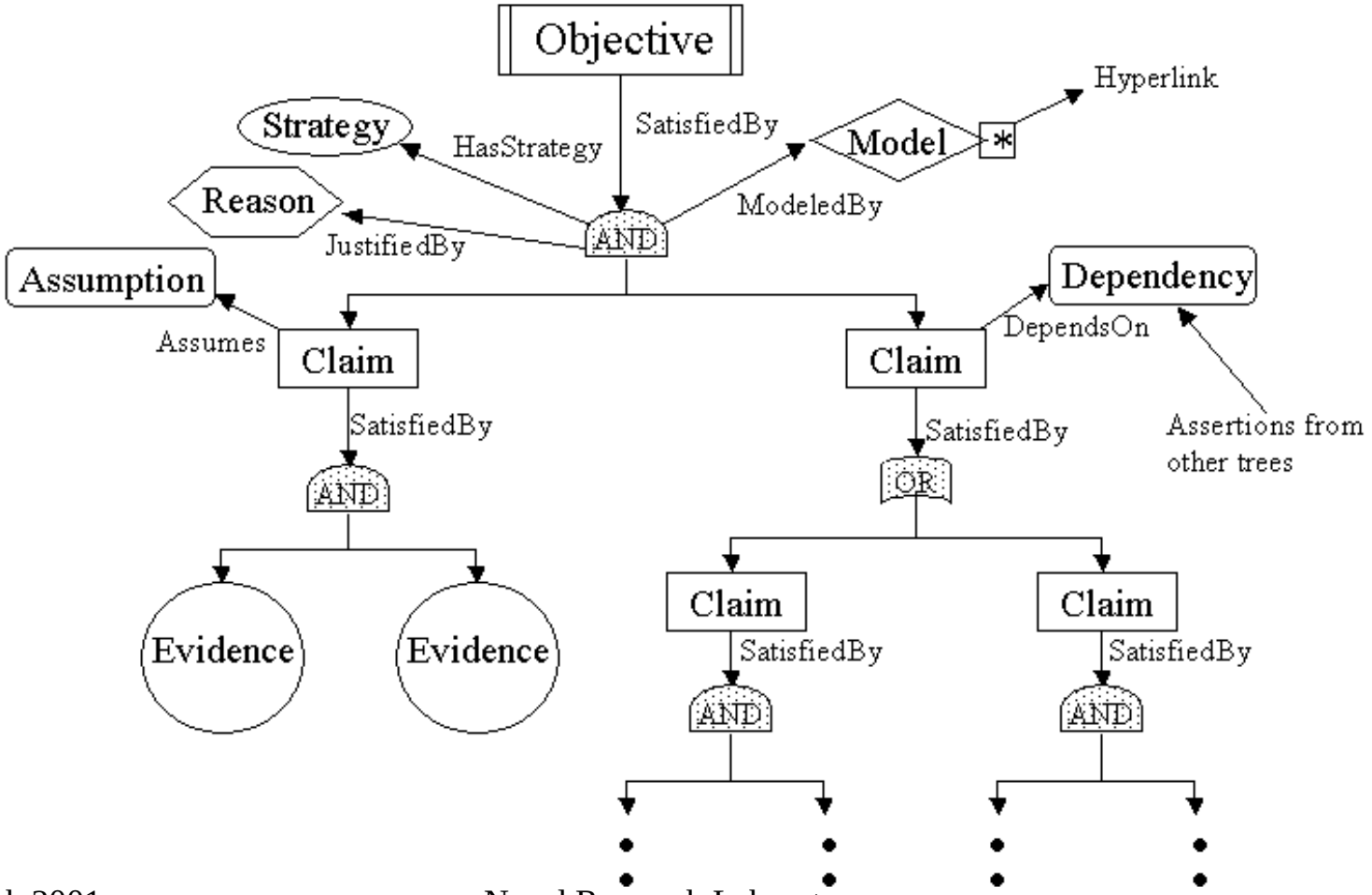
Enterprise Certification Methodology (ECM)

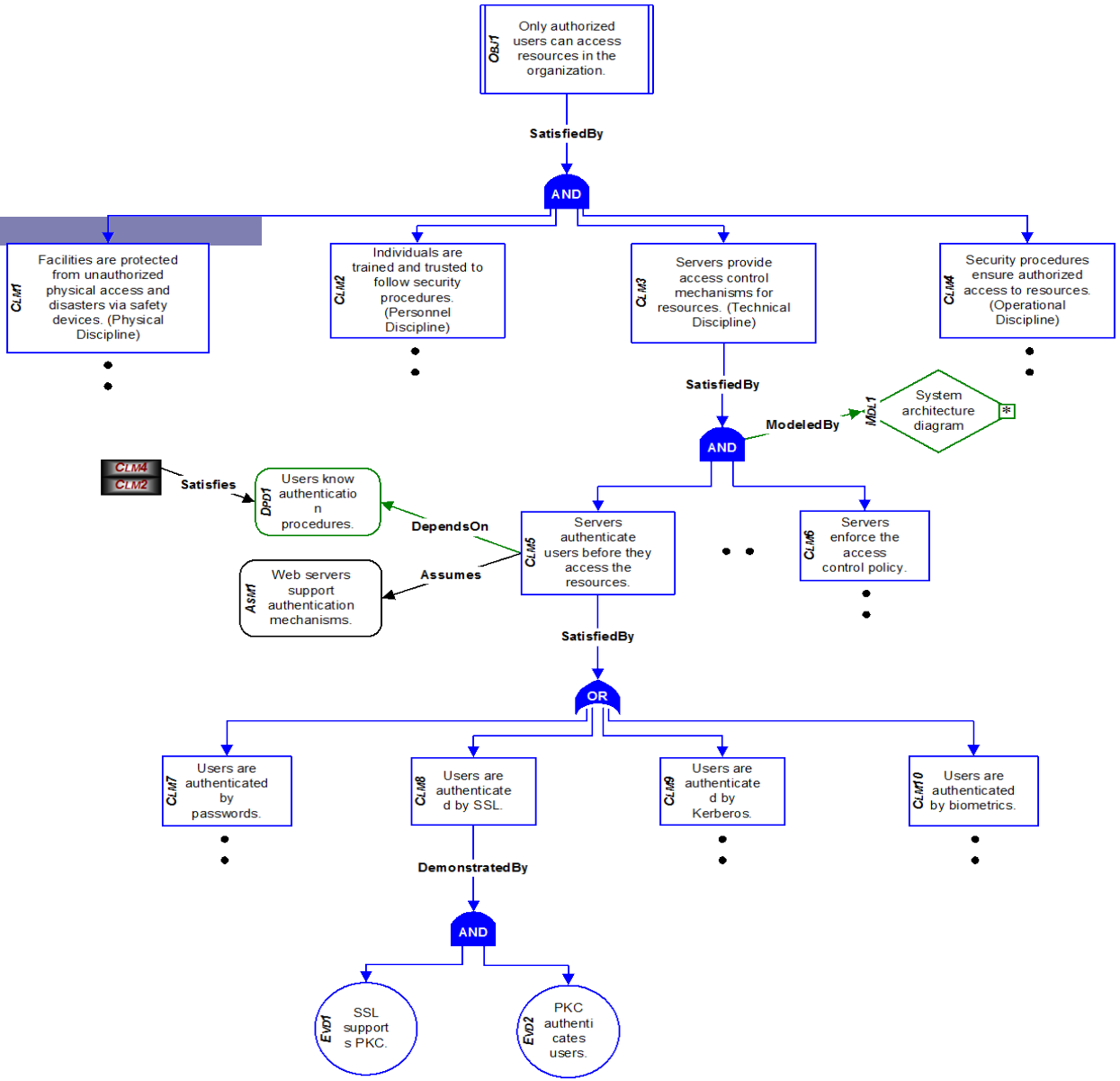
- Four disciplines (NSA's NRM)
  - Physical, personnel, technical, and operational disciplines
- Dependencies between assumptions and assertions (NRL's Assurance Strategy)
  - An assumption in one claim tree
    - Can be validated by assertions in other trees
    - Without validation ➔ Vulnerability

Composite Assurance Mapping Language (CAML)

- Developed by merging and extending GSN and MOAT for visual notations
- Describes assurance arguments in a well-organized map
  - Common language for designers and assessors
  - Supports diverse sources for evidence
  - Makes dependencies explicit
  - Supports life cycle assurance for systems
  - Supports re-certification of systems

CAML Structure and Primitives




OBJ1
Only authorized users can access resources in the organization.
SatisfiedBy
AND
CLM1
Facilities are protected from unauthorized physical access and disasters via safety devices. (Physical Discipline)
CLM2
Individuals are trained and trusted to follow security procedures. (Personnel Discipline)
CLM3
Servers provide access control mechanisms for resources. (Technical Discipline)
CLM4
Security procedures ensure authorized access to resources. (Operational Discipline)
SatisfiedBy
ModeledBy
MDL1
System architecture diagram
AND
CLM4
CLM2
Satisfies
DPD1
Users know authentication procedures.
DependsOn
Assumes
ASM1
Web servers support authentication mechanisms.
CLM5
Servers authenticate users before they access the resources.
CLM6
Servers enforce the access control policy.
SatisfiedBy
OR
CLM7
Users are authenticated by passwords.
CLM8
Users are authenticated by SSL.
CLM9
Users are authenticated by Kerberos.
CLM10
Users are authenticated by biometrics.
DemonstratedBy
AND
EVD1
SSL supports PKC.
EVD2
PKC authenticates users.

Tools

- Visual Network Rating Methodology (VNRM)
- Security Assurance Navigation Environment (SANE)

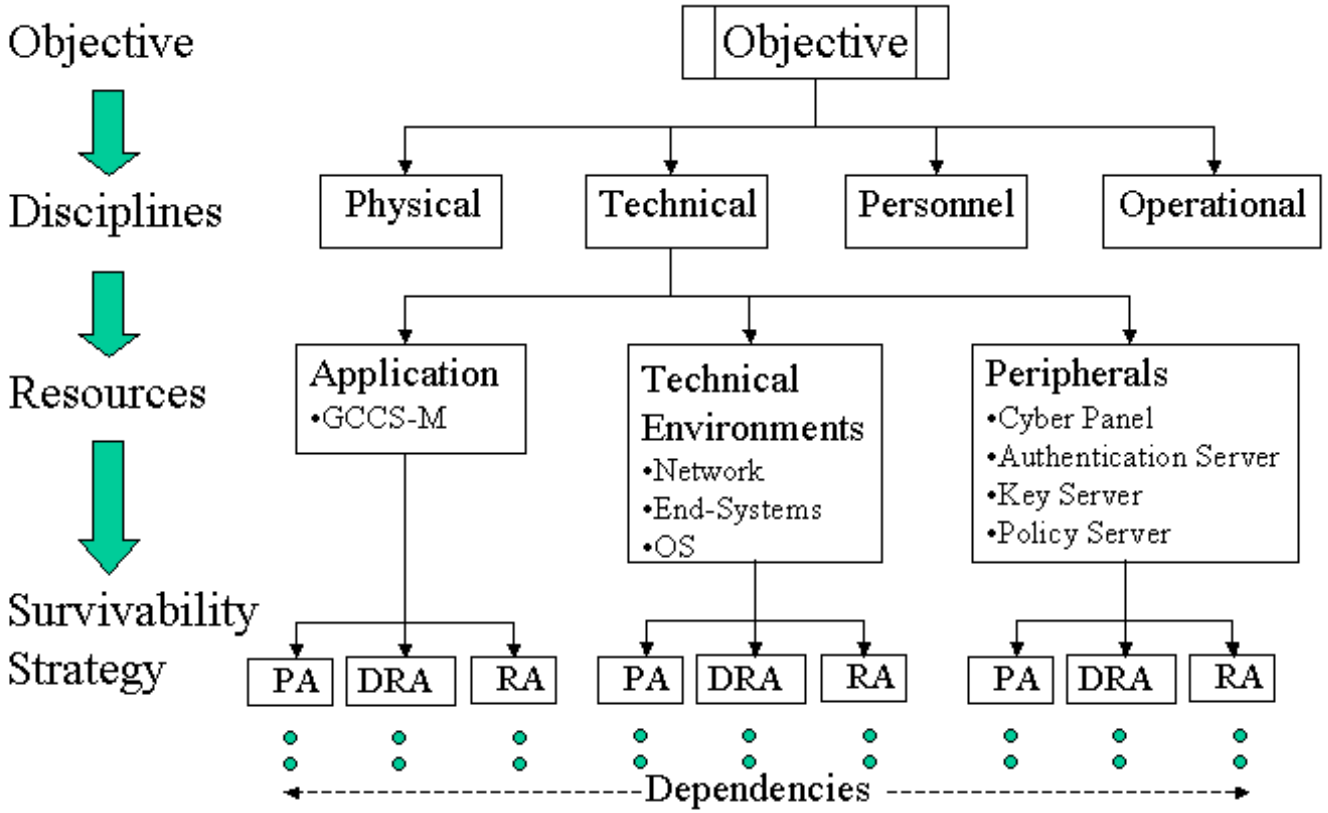
Visual Network Rating Methodology (VNRM)

- A prototype toolset
  - Developed in Visual Basic
- Helps users
  - Draw a graphical assurance map in CAML based on ECM
  - Document related descriptions.
- Integrated with external programs
  - MS Word, Visio, Access
- Not standalone

Visual Network Rating Methodology (VNRM)

- Use Cases
  - OO-DTE (Object-Oriented Domain-Type Enforcement, NAI Lab)
  - ARGuE (Advanced Research Guard for Experimentation, NAI Lab)
  - VPN implementation (DARPA)
  - Survivable GIG (Global Information Grid, DoD)
  - ELB (Extending Littoral Battlespace)

Hierarchical Assurance Strategy for Survivable GIG



*PA: Prevention Arguments
*DRA: Detection & Response Arguments
*RA: Recovery Arguments

Extending the Littoral Battlespace ACTD

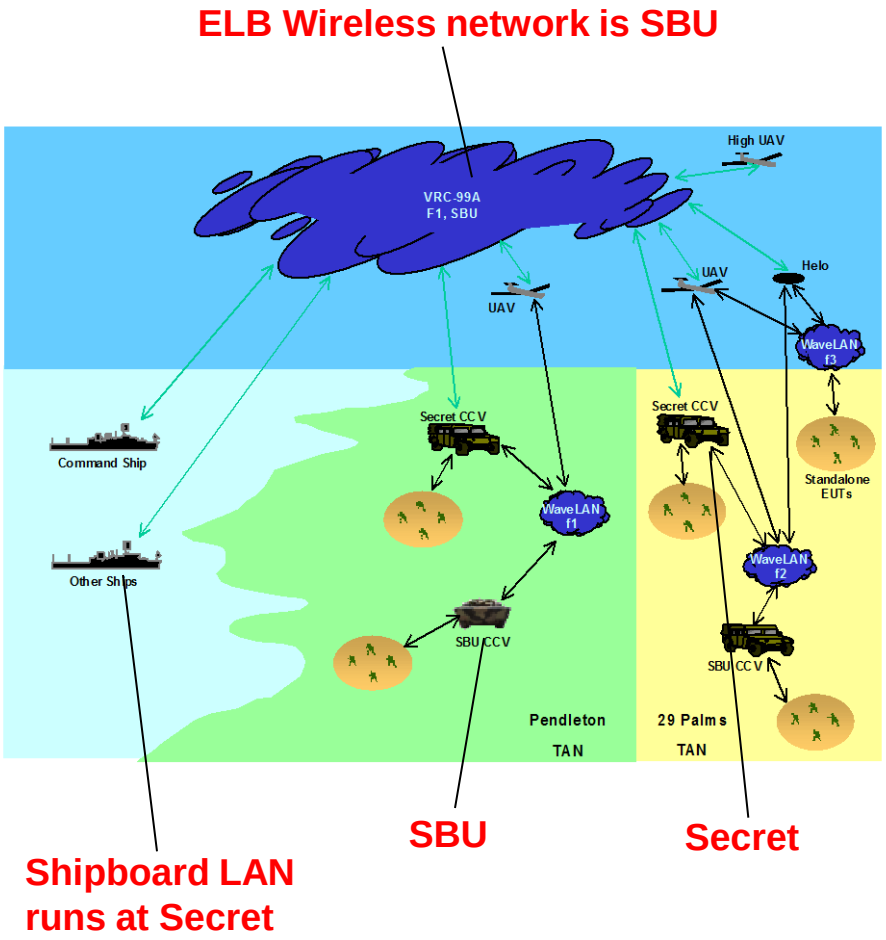
Security for Wireless Ship-Marine Communication

Objective: **Protect confidentiality, integrity, and availability of sensitive information to both Navy and Marine Corps**

- **Allow SBU Marine wireless network to connect to Navy Secret shipboard net**

Approach: **Use MSL architecture with Radiant Mercury as boundary controller and firewalls as enclave controllers**

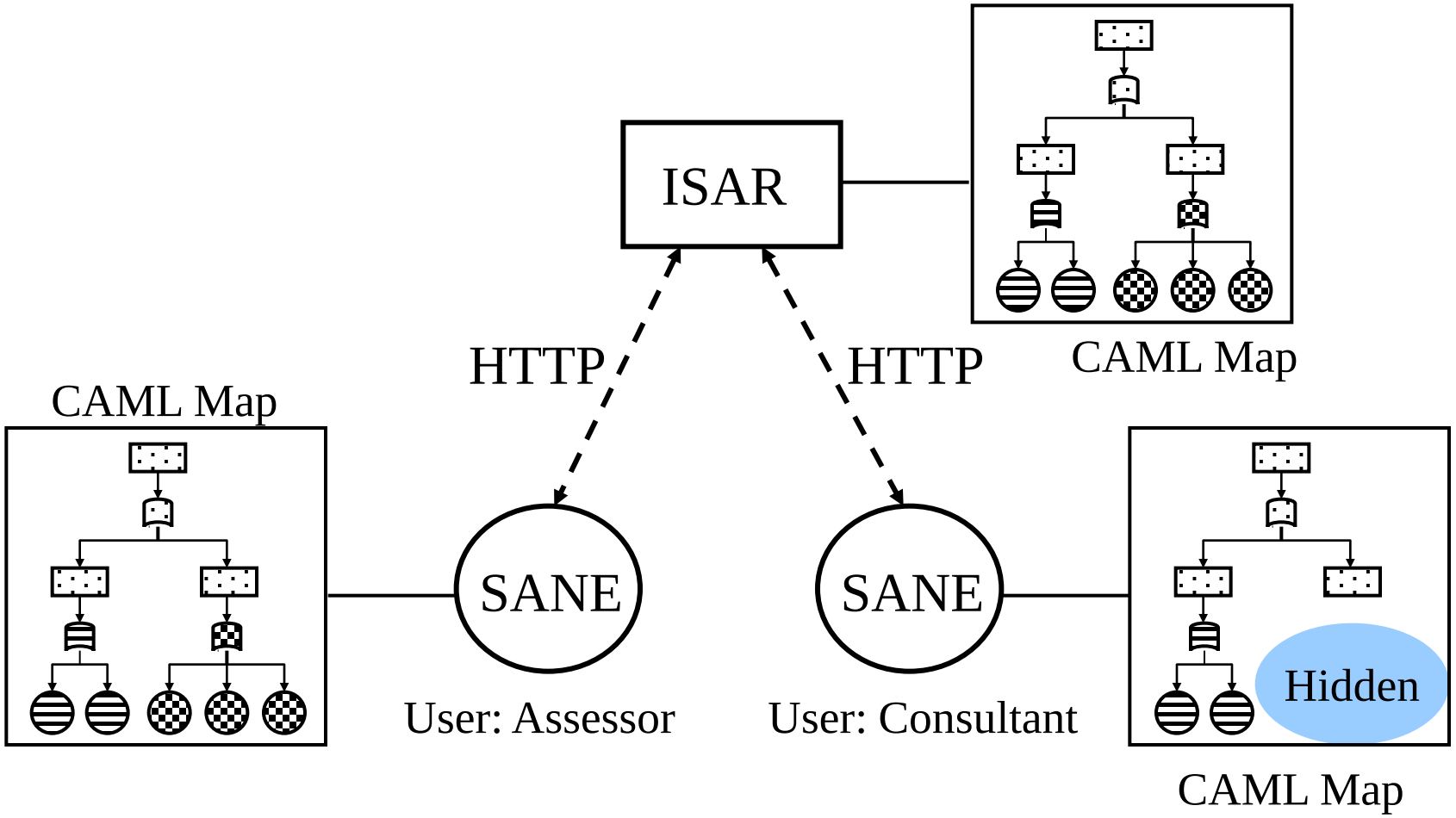
- **Separate information at different classification levels in transit with Type 1 encryption**
- **Provide identification and authentication mechanisms, and network intrusion detection**



Security Assurance Navigation Environment (SANE)

- Standalone toolset
  - Developed purely in JAVA
- Supports what VNRM does
- New features
  - Supports cooperation and reusability of CAML maps via the Information Security Assurance Repository (ISAR) on the Web
  - Supports access control to CAML maps based on users' roles

Security Assurance Navigation Environment (SANE)



Accomplishments

- We have introduced the concept of an assurance argument map
- We have developed
  - A methodology (ECM)
    - To compose and organize comprehensive assurance arguments and create a roadmap for linking different kinds of assurance evidence
    - A Language (CAML)
    - To describe a map of assurance arguments
  - Tools (VNRM, SANE)
    - To help users develop the assurance argument maps in CAML based on ECM

Enhancement

- CAML can be integrated with existing technologies
  - Common Criteria
  - Formal methods
  - UML (Unified Modeling Language)
  - Countermeasure Characterizations
  - ETC.

Future Work

- Finish SANE development
- Catalog the sets of CAML maps
- Extract argument patterns (strategies) for recurring solutions
- Populate ISAR with reusable information

Impact

- Improved information security design by enabling better design tradeoff analysis
- Promotes comprehensive, multidiscipline view of assurance
- Provides hyperlinked index into the assurance evidence
- Reduced lifecycle cost through reuse of independently developed components and their assurance arguments in composite systems
- Increased objectivity of system certification and accreditation decisions
  - **Explicit identification of vulnerabilities**
  - **Improved understanding of risks by management and operational approval authority**

References

- 1. Joon S. Park and Judith N. Froscher, Tools for Information Security Assurance Arguments, 2nd DARPA (The U.S. Defense Advanced Research Projects Agency) Information Survivability Conference and Exposition (DISCEX II), Anaheim, California, June 12-14, 2001.
- 2. Joon S. Park, Andrew Moore, Bruce Montrose, Beth Strohmayer, and Judith N. Froscher, A Language, a Methodology, and a Tool to Provide Information Security Assurance Arguments, will be submitted to 8th ACM Conference on Computer and Communications Security (CCS-8), Philadelphia, Pennsylvania, November 6-8, 2001.
- 3. Andrew Moore, Bruce Montrose, and Beth Strohmayer. A Tool for Mapping Enterprise Security Assurance. Technical Report 5540-051a:apm, Naval Research Laboratory, September 2000.
- 4. Andrew Moore and B. Strohmayer. Visual NRM User's Mannual. Technical Report NRL/FR/5540--00-9950, Naval Research Laboratory, May 2000.
- 5. VNRM (Visual Network Rating Methodology): Tools for Mapping Assurance Arguments. http://chacs.nrl.navy.mil/projects/VisualNRM/, Naval Research Laboratory, 2000.