Naval Information Warfare Center PACIFIC

A Pattern-based Methodology for Modeling Investigations in CFTaaS Architectures

26 April 2022

Juan C Bennett, Ph.D.

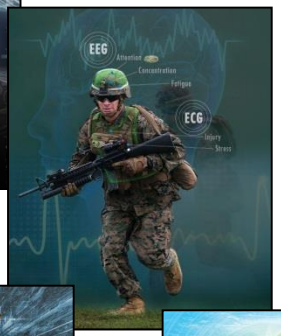
SSC PACIFIC CFRL CYBER FORENSICS RESEARCH LAB

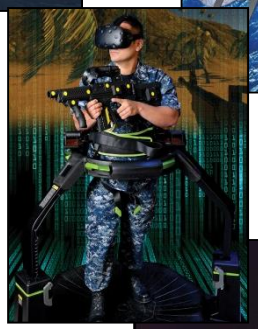
Naval Information Warfare Center PACIFIC

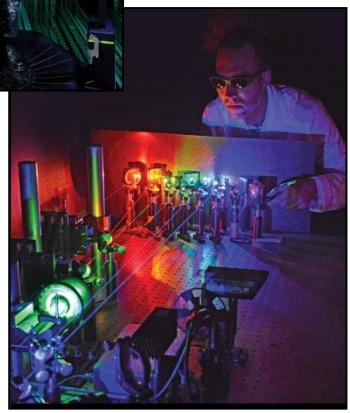
NIWC PAC MISSION

SSC PACIFIC CFRL CYBER FORENSICS RESEARCH LAB

From concept to capability via…







…research, development, engineering, and support of integrated C4ISR, cyber, and space systems across all warfighting domains

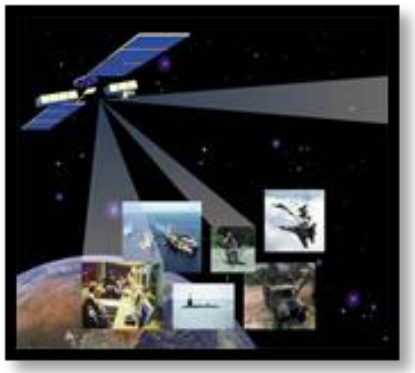
Naval Information Warfare Center PACIFIC

Cyber Forensics Research Lab (CFRL)

SSC PACIFIC CFRL CYBER FORENSICS RESEARCH LAB

Mission

- Investigate novel ways to collect, protect, analyze network-based evidence.
- Understand collection, classification/exploitation of knowledge about adversaries (cyber threat intelligence) from a cyber-forensics perspective.
- Perform network forensics investigations in different DoD environments (e.g. cloud-based, mobile, converged, tactical), analyze traffic and flow records, behavior analysis, and generate intelligence.
- Platform for investigating network attacks and training our engineers and scientists
- Research collaboration with industry, academia and government.

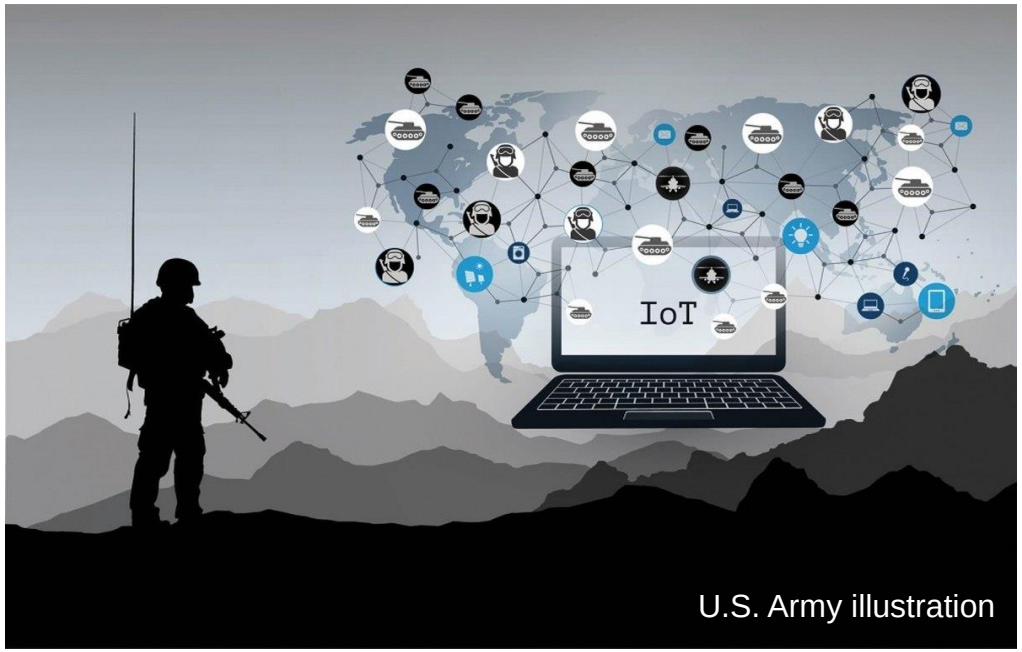


Operational Relevance

- Enables DCO forces to detect incidents across multiple Navy networks
- Allows DCO forces to conduct network monitoring and analysis within a converged environment
- Develop novel forensic tools and methods to conduct live cyber forensic investigations
- Support network investigators to identify actual intrusions, collect more and better evidence, reduce analysis time, and help to stop attacks against the converged network.
- Improving cyber posture for immediate and persistent cyber threats to networks
- Reduction in threat detection to response time
- Reduction in Cyber Analyst Information Overload

Internet of Battlefield Things (IoBT)

- Growth of smart infra-structure, cloud and IoT devices added more attack surfaces.
- It's expensive to build cyber forensics testbeds and gain expertise in the field
- Need for a federated testbed to integrate isolated testbeds.
- Emerging UC/5G technologies as key future communication platforms



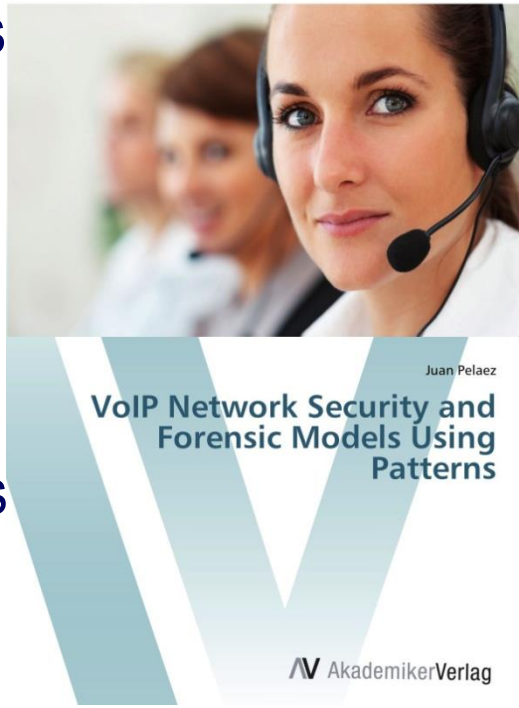
U.S. Army illustration

Naval Information Warfare Center PACIFIC

Secure Systems Development Methodology

SSC PACIFIC CFRL CYBER FORENSICS RESEARCH LAB

- OO models can be converted into software.
- Dynamic aspects of model can be implemented as ops classes and the data parts of a class can be mapped to relational databases.
- UML accepted standard for s/w development. UML visual language appropriate for description of system architecture.
- Software patterns are established for software analysis design to improve reusability and reliability.
- Approach combines UML and patterns to present models and mechanisms for security and forensics.
- Patterns used to build or evaluate secure systems or for teaching security (UDEL ELEG/CPEG 467-667, Introduction to Network Security)



Naval Information Warfare Center PACIFIC

Network Models Using Patterns

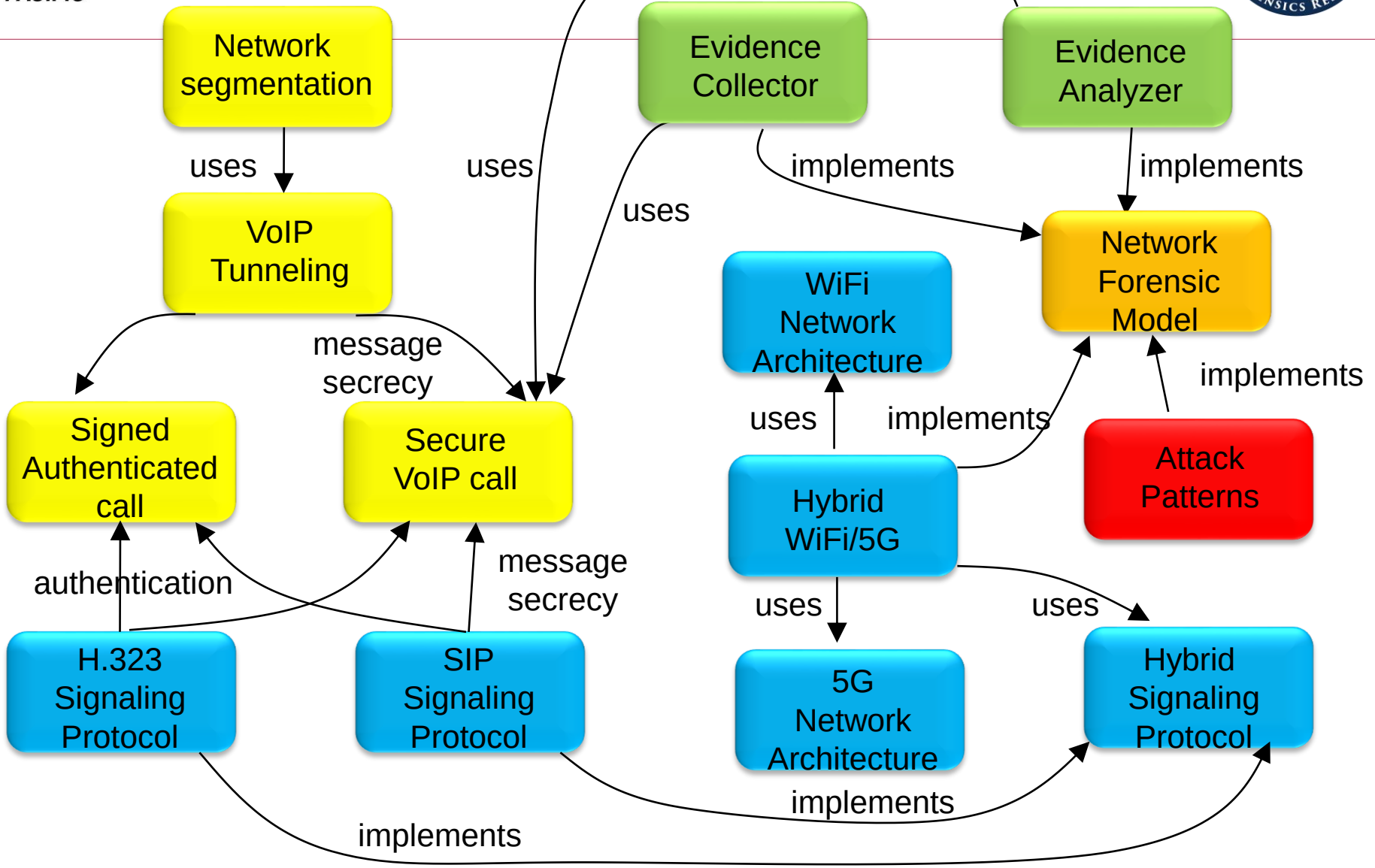
- Discover new ways to characterize network environments and information embedded in the network.
- Comprehensive pattern system based on a collection of semi-formal patterns.
- Analyze network forensic investigations in converged environments using forensic patterns.
- Pattern systems specify, analyze and implement network forensics investigations for different architectures.
- Secure and convenient method of collecting/analyzing digital attack evidence in converged environments.

Naval Information Warfare Center PACIFIC

UC Pattern System

- **Architectural patterns**
  - Analyze cloud-based converged architectures in UC**.**
  - Focus on modeling enterprise architectures using semi-formal models.
  - Patterns are used for high-level specification of the UC system.
- **Attack patterns**
  - Systematic description of the steps/goals of an attack and ways to defend and trace its application in a system.
  - Attack pattern template to describe how to document and organize generic attack patterns.
  - Attack pattern catalog.
- **Security patterns**
  - Based on security mechanisms/standards to stop attacks against the UC system.
  - Understand what security patterns are necessary to prevent or mitigate the threats.
- **Forensic patterns**
  - Capturing, recording, and analyzing information collected on UC networks from several intrusion detection, auditing, and checking points.
  - Help network investigators to select relevant evidence

UC Pattern System



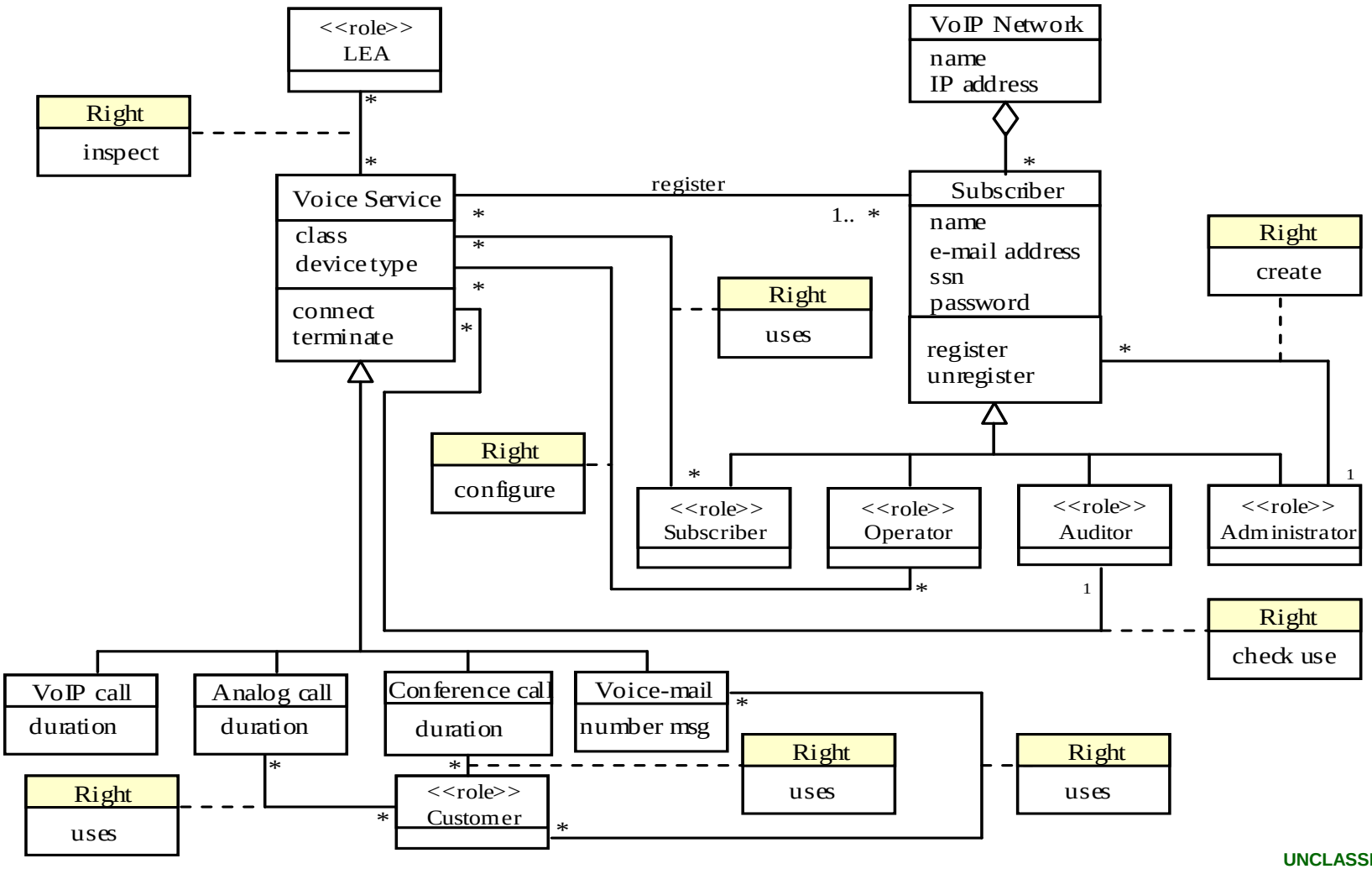
Naval Information Warfare Center PACIFIC

Network Forensics Patterns

- Network forensics adds another dimension of protection to the system.
- Need for systems that allow not only the detection of complex attacks, but understanding the attack, and collecting enough evidence of these crimes.
- The collection of media packets in real time and the use of automatic mechanisms are fundamental.
- Forensic Patterns provide an abstract view of forensic information to network investigators.
- Goal: enable a faster response and more structured investigations of network attacks.
- Discover the source of security breaches

Naval Information Warfare Center PACIFIC

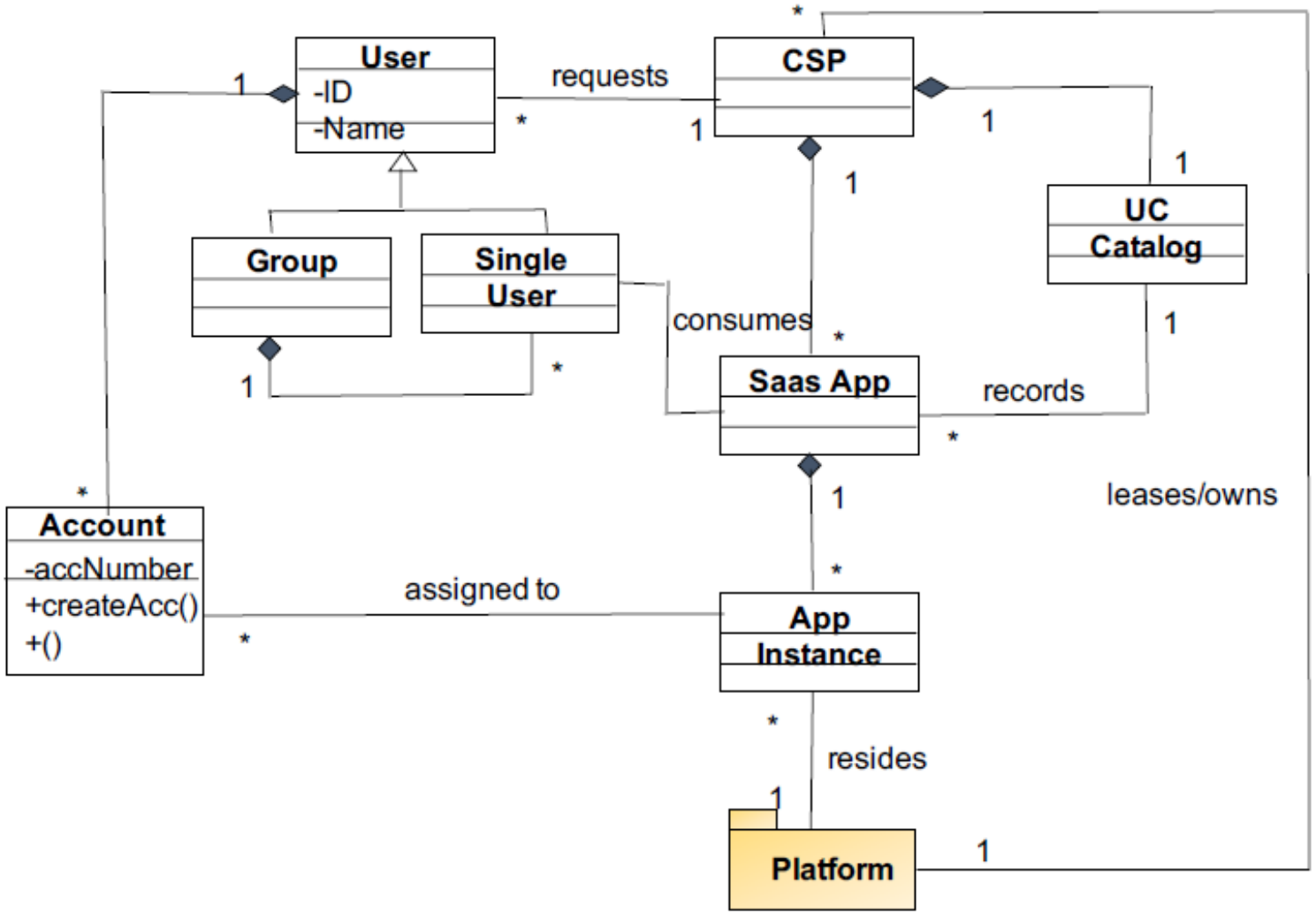
Roles and Rights in UCaaS Model



UNCLASSIFIED

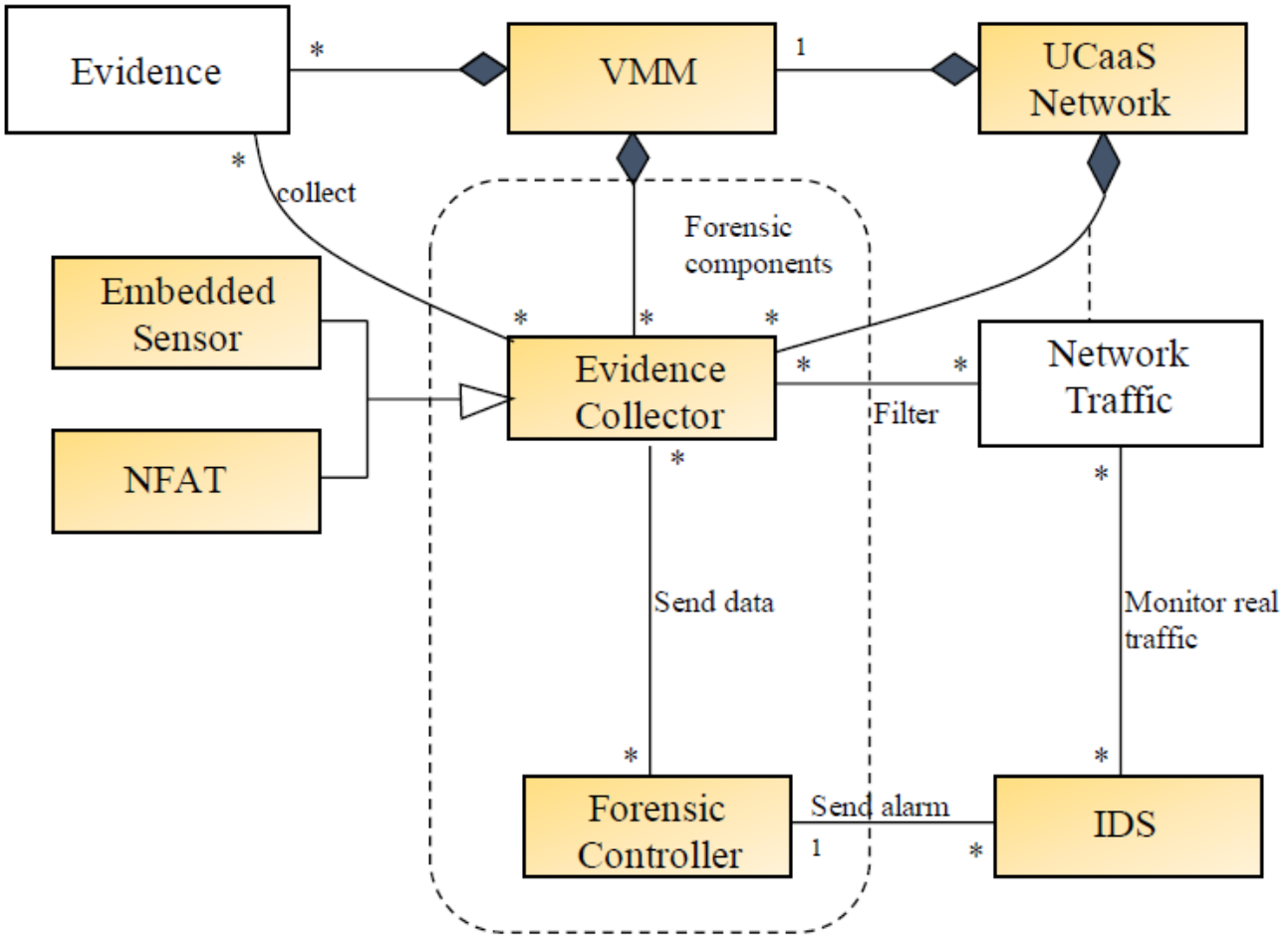
Naval Information Warfare Center PACIFIC

Class Diagram for UCaaS Pattern

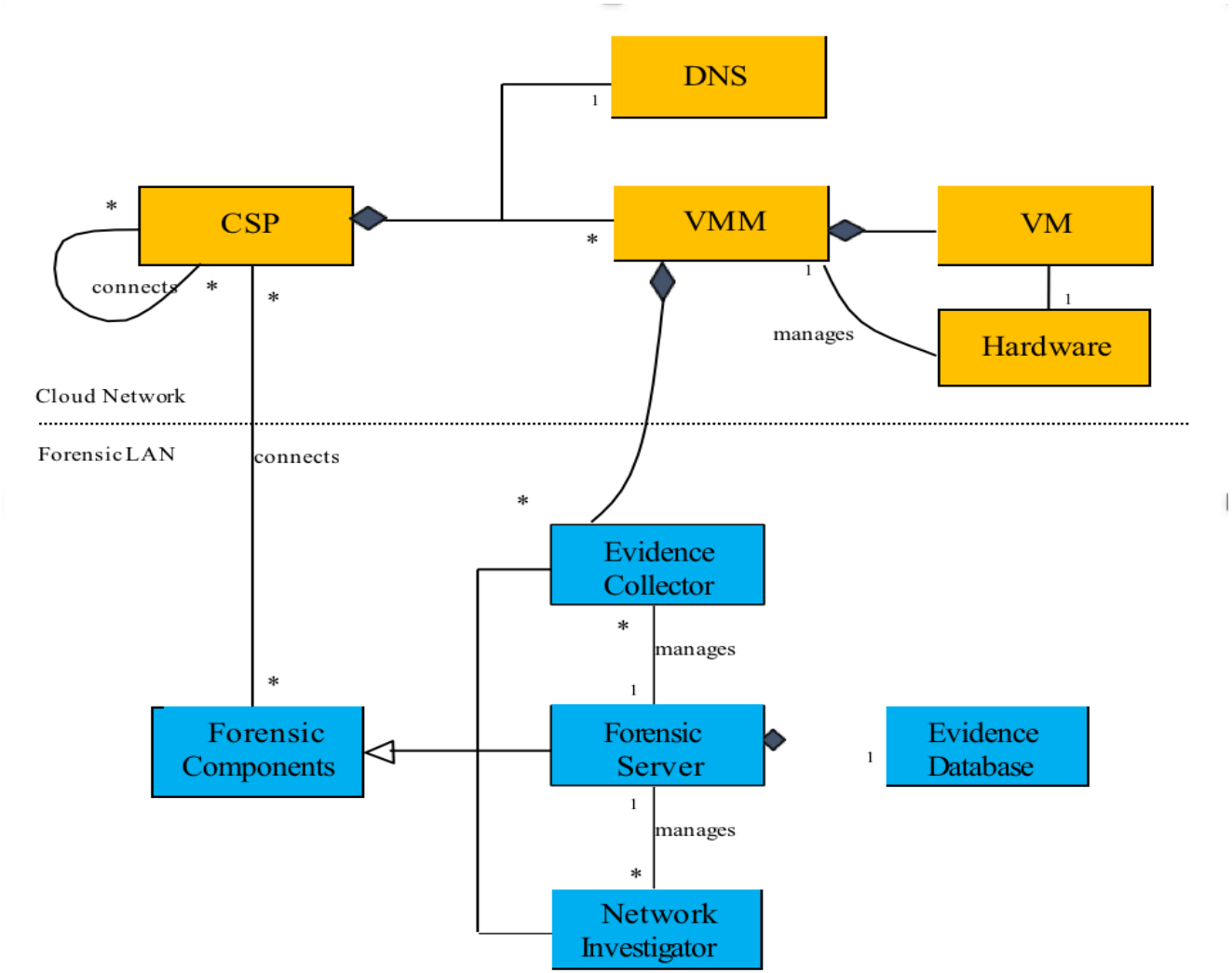


Naval Information Warfare Center PACIFIC

Cloud Evidence Collector



Simplified Cloud Forensic System Architecture



Naval Information Warfare Center PACIFIC

Cloud Forensics System

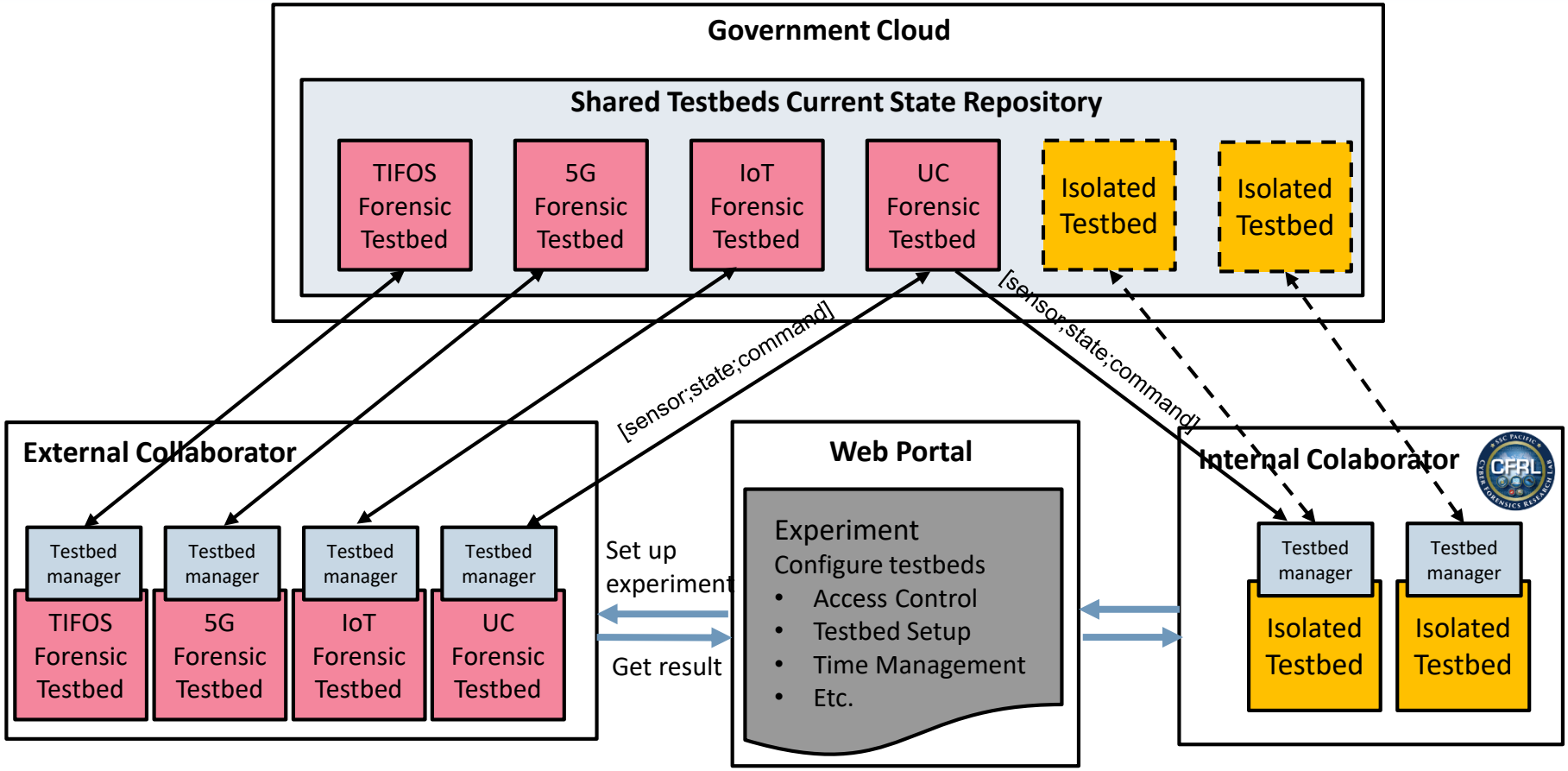
- Develop autonomic UCaaS forensic system including novel forensic tools and methods to conduct live forensic investigations.
  - Expand existing cyber forensic capabilities at CFRL.
  - Testbed to include set of voice, video and data-sharing capabilities
  - Complexity/dynamic behavior of converged network systems
- Analyze the identification, collection and analysis of forensic evidence in converged cloud environments (VVoIP).
- Develop UCaaS testbed to create high-fidelity simulations of existing and future Navy communications architectures.

Naval Information Warfare Center PACIFIC

CFTaaS Objective

- Develop cloud-based system to experiment with and evaluate different tools and techniques to detect, collect and analyze forensic evidence in near real-time.
- Develop federated cyber forensic testbed to evaluate different cyber forensic techniques and tools to detect and protect enterprise infrastructures and their services
- Analyze the identification, collection and analysis of forensic evidence to address the next domain of cloud forensics.
- CFTaaS system designed to provide self-defense mechanisms (immune) against non-self (i.e., malicious intruders) within a cloud environment for optimized approach.
- Protect smart infrastructures and their services from malicious cyberattacks, faults or accidents.
- Support network investigators to identify actual intrusions, collect more and better evidence, reduce analysis time, and help to stop attacks against the enterprise network.

CFTaaS Concept Architecture



Naval Information Warfare Center PACIFIC

CFTaaS Benefits

- Develop innovative training cyber forensic experiments, provide hands-on experiences.
- Provide service oriented architecture to publish forensic and security experiments for research and training.
- Automated method for identification, collection and analysis of forensic data to conduct live cyber forensic investigations.
- Access geographically dispersed heterogeneous testbeds and maintain privacy of users and their experiments running on cross-domain resources.
- Explore innovative techniques to overcome research challenges of developing a multi-domain collaborative and federated cyber forensic testbed environment.

Naval Information Warfare Center PACIFIC

Conclusions

- Model-based CFTaaS approach lays the foundation for future practical work.
- Automation increases forensic soundness of the data-acquisition process by making it repeatable and not dependent upon manual and possibly error-prone human interactions.
- Implement live forensics as a secure and convenient method of collecting/analyzing digital evidence in converged environments.
- Patterns can guide systems development, be used to evaluate existing designs, be a basis for simulation, and be a pedagogical tool.
- Creation of a comprehensive pattern system to be used in forensic investigation processes.
- Concentrated on pattern functionality/usefulness. First steps toward a methodology for modeling digital forensics.
- Potential to be used as evidence. Forensic patterns value may be realized when semi-formal models are reused on similar investigations.
- Semiformal models introduced to address unique challenges of digital forensics based on sound principles but still require extensive scientific validation in practice.

Moving Forward

- Strong demand for Cyber security and forensics
- Development of automated network forensic systems using modeling and simulation approaches.
- Collaborations with other disciplines to develop new tools enhance existing forensic frameworks.
- Analyze new and evolving network attacks. Expand attack pattern catalog.
- Design new tools for better evidence collection/analysis (e.g. network behavior analysis).
- Proactive vs. reactive network
- Live-forensics vs. post-mortem
- Innovate, Integrate, Interoperate

Naval Information
Warfare Center

PACIFIC