SPAWAR
Systems Center
PACIFIC

A Semiformal Forensics Approach to UCaaS Architectures

16 October 2018

SSC PACIFIC
CFRL
CYBER FORENSICS RESEARCH LAB

Juan C Bennett, Ph.D.

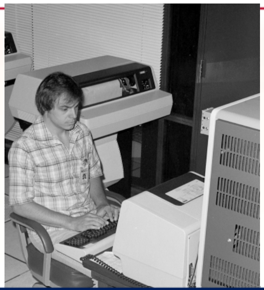
SPAWAR
Systems Center
PACIFIC

SSC PAC: A Legacy of Discovery for 75 Years

SSC PACIFIC · CFRL · CYBER FORENSICS RESEARCH LAB

Arctic Submarine Operations

Radar / EW


ARPANET

Celebrating Seventy Five Years on the Point
75 years
SPAWAR Systems Center Pacific

Personalized Assistant that Learns (PAL)

NTDS

Laser Research

Polaris

SHF SATCOM

Underwater Acoustics

Ship-launched Torpedoes

Distribution A: Approved for public release; distribution is unlimited.

Capabilities – Across the Full Life Cycle

Today
The Navy in Operation

Installation and Support

Tomorrow
The Navy in Construction

Engineering, Development, Test and Evaluation

Future
The Navy in Planning

Science and Technology

Production, Installation In-Service Support

Marine Mammals

Networks

3D Printing/ AM

Cyber Security

C4ISR for Unmanned Vehicles

Afloat Mobility

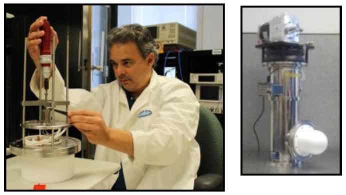
Integrated Fires

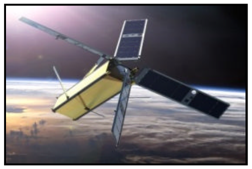
Electronic Warfare Battle Management

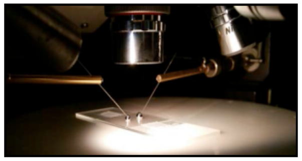
Integrated Cyber Operations

Space Command & Control

User Center Design


Cryogenic Exploitation of RF (CERF)


Nano Satellites


Graphene

Mixed Reality

Human Autonomy Teaming

Advanced Antenna Research

SPAWAR

Systems Center
PACIFIC

SSC PAC MISSION

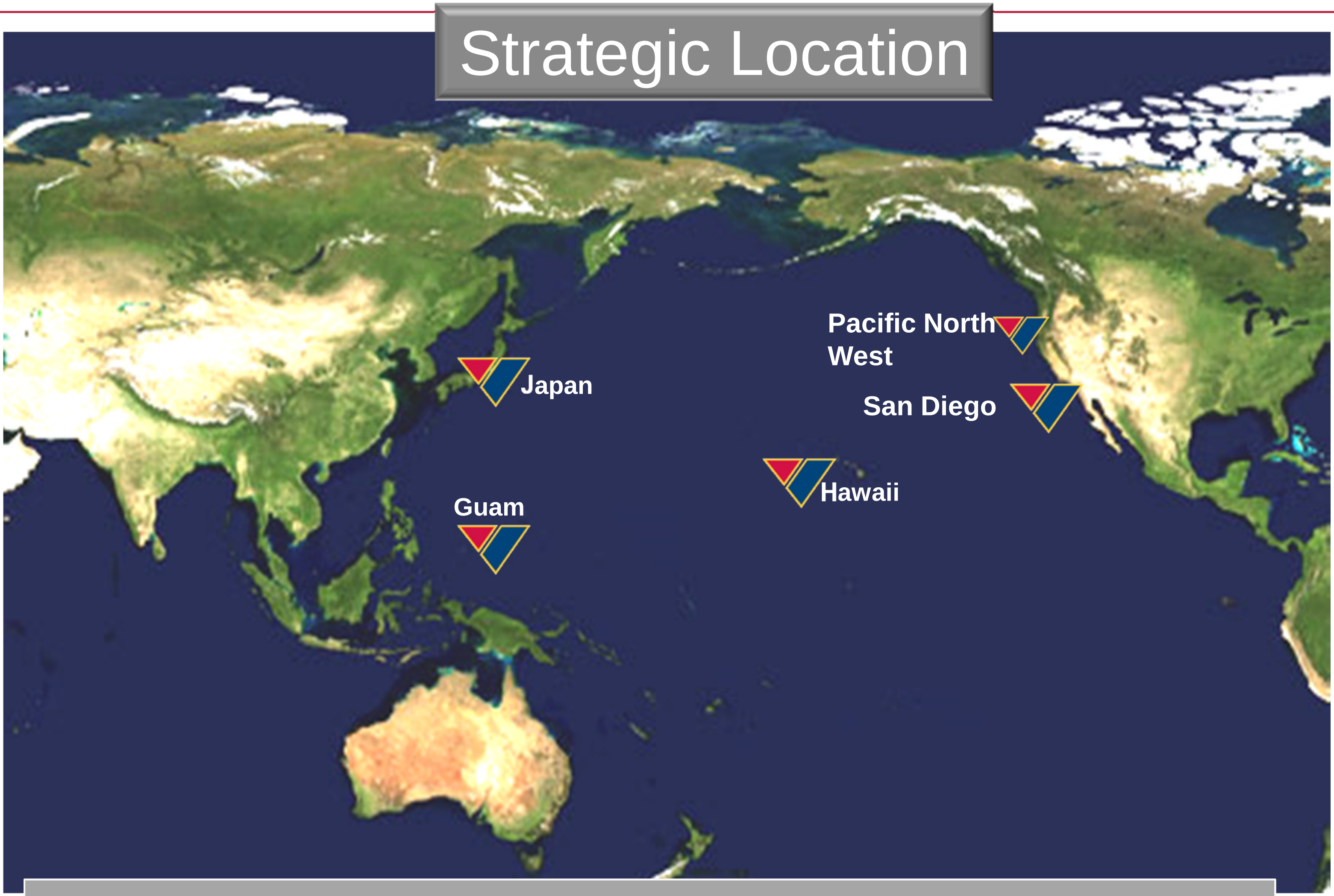
SSC PACIFIC
CFRL
CYBER FORENSICS RESEARCH LAB

From concept to capability via…

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

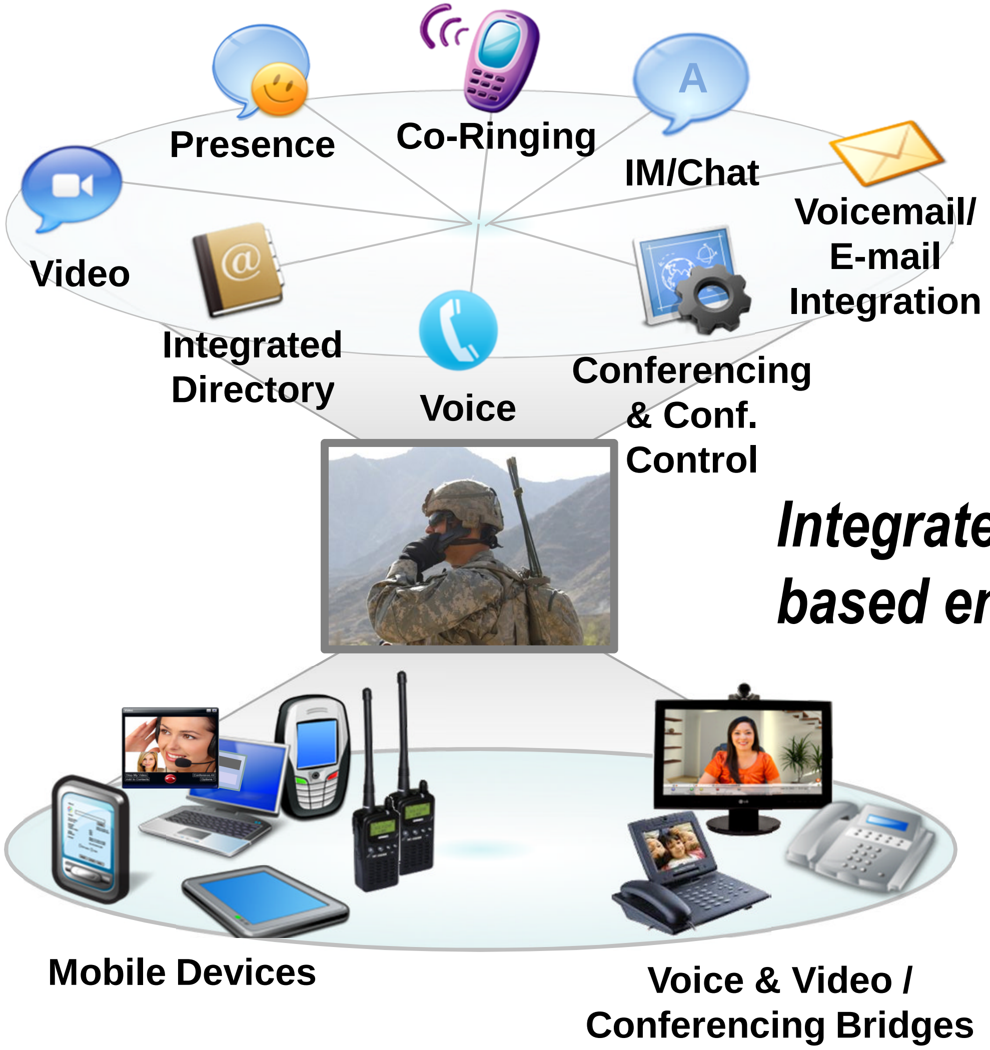
SSC PAC Support in the Pacific Region

Strategic Location



Only DoD Lab Located in a Major Fleet Concentration Area

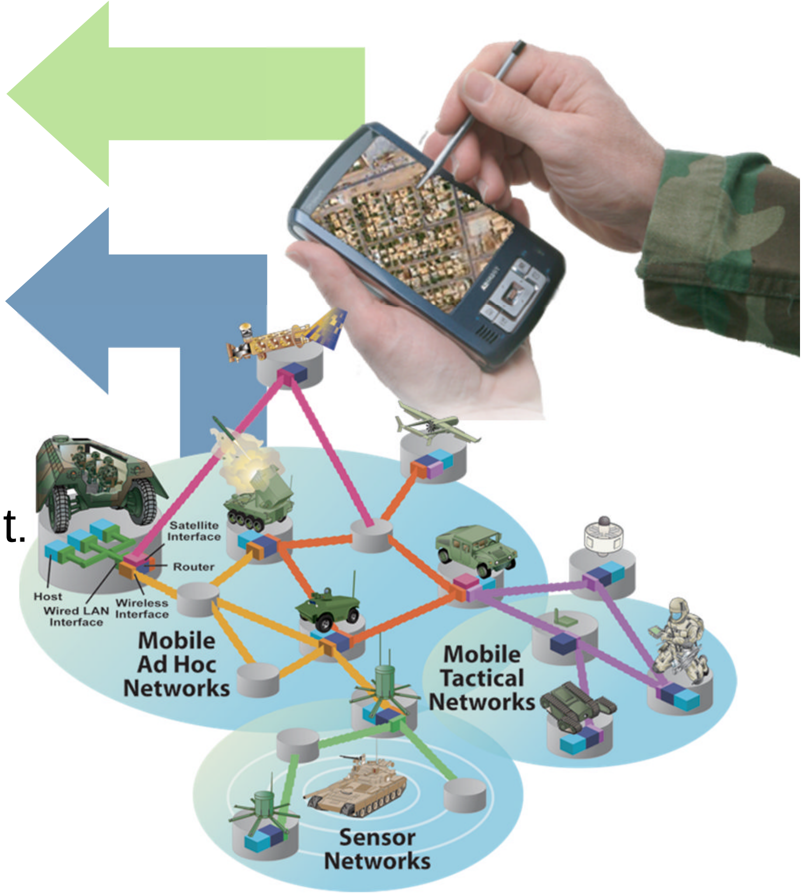
Unified Capabilities


Presence
Co-Ringing
IM/Chat
Voicemail/ E-mail Integration
Video
Integrated Directory
Voice
Conferencing & Conf. Control
Mobile Devices
Voice & Video / Conferencing Bridges

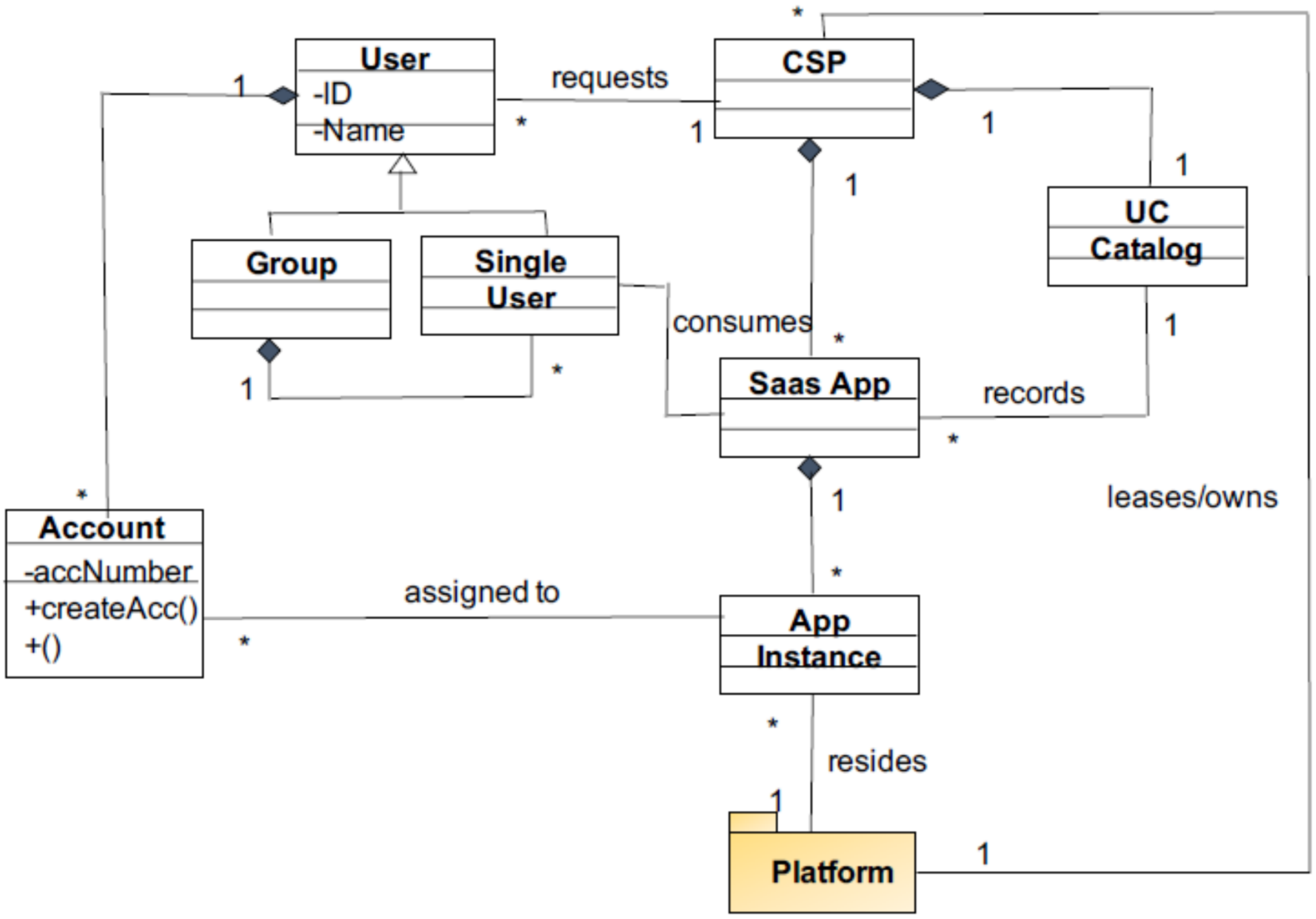
Integrated, fully-converged, cloud-based environment

Network Architecture Challenges

- H.323 and SIP protocols for signaling and call control in VoIP.
- Provide total access and supporting IP svc.
- H.323 is complex, requires a combination of components to perform.
- Current UC deployments are based on legacy technology
- End of life for circuit switched technologies
- Need high-level specification of the UC architecture that can be used to conduct forensic investigations in a tactical environment.
- Analyze the interoperability with other multimedia service networks and terminals.
- Users limited control over SaaS infrastructure



Class Diagram for UCaaS Pattern



Digital Forensics Overview

- **Digital Forensics**
  - Investigate attacks in networked systems and applications
  - Example Tools:
    - Instruction detection systems - IDSs (e.g. Snort, AIDE)
    - Packet capture tools (e.g. Tcpdump)
    - Network data collectors (e.g. NFAT)
- **Process**
  - Identify, collect and analyze forensic evidence from the network
  - Reconstruct network attacking behavior using raw data
  - Isolate the specific incidents and identify attackers

Network Forensic Challenges -Collection-

Forces

- Firewalls and IDS, cannot detect or prevent all attacks.
- Manual analysis not possible. Forensic methods with shorter response times needed.
- Systematic approach needed to detect vulnerabilities/resulting attacks.
- Need network models to detect complex attacks in tactical environments
- VoIP, requires automated collection of forensic data to provide data reduction/correlation.
- CSP control system and applications provided by the system
- Data replication, location transparency, and multi-tenancy are unique to cloud computing forensics.
- Complex systems difficult to monitor, protect and analyze due to many factors such as size, architecture complexity, distributed nature, heterogeneity, the large numbers of users, and diversity of services provided

Network Forensic Challenges –Analysis-

Forces

- Analysis and reconstruction of attacks time-consuming and human-intensive tasks.
- Storing network data for forensic analysis may be complicated.
- Encrypted packets are difficult to analyze.
- Forensic analysis process must guarantee data preservation and integrity.
- Attacks in converged networks becoming more frequent/complex to counter.
- Lack of experience executing investigations or using similar forensic tools.
- Dynamic behavior, and availability of many heterogeneous devices
- Structured method required for reusing cloud forensic knowledge and documenting forensic investigations.
- Forensic tools incapable to accurately characterize current states, detect malicious attacks, and stop them or their fast propagation and/or minimize their impacts.

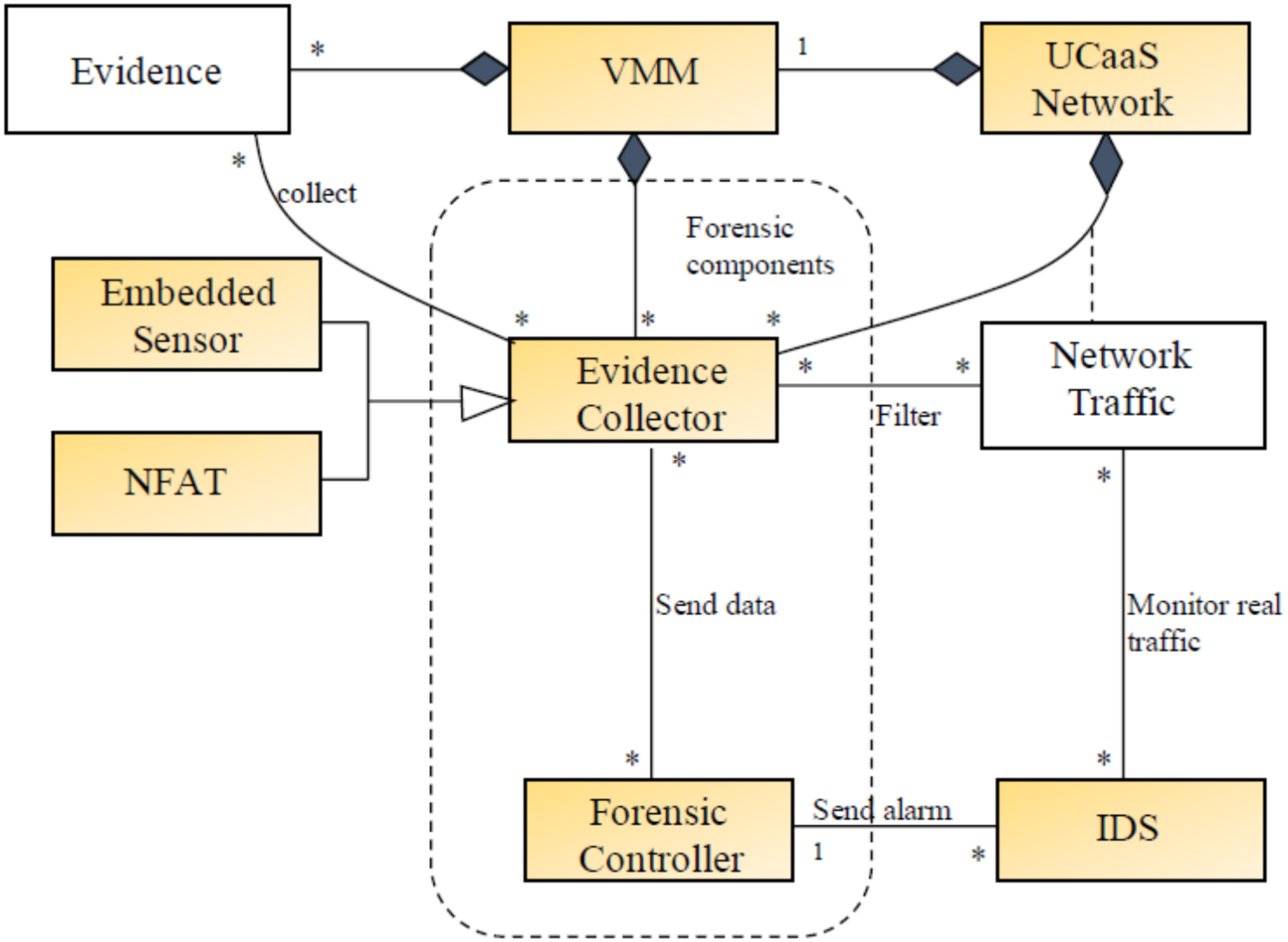
Network Models Using Patterns

- 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.

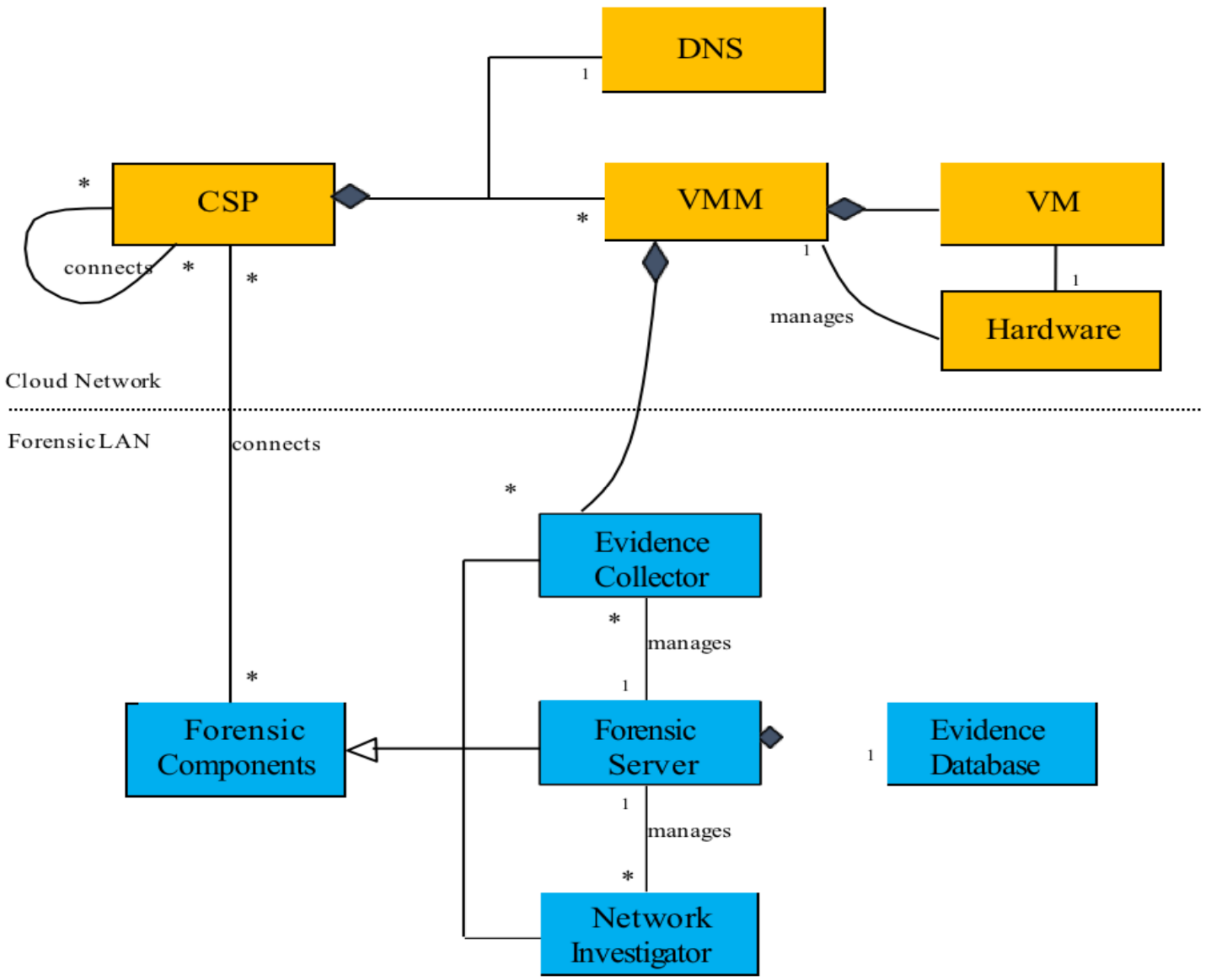
Network Forensics Patterns

- Extra dimension of protection to the system.
- Abstract view of forensic information to network investigators.
- Enable faster response and more structured investigations of network attacks.
- Discover source of security breaches
- CEC to collect attack packets on the basis of adaptively setting filtering rules for real-time collection.
- Sensors with examination capabilities to look at UC traffic (i.e. signaling and media)
- CEA analyzes collected forensic data packets, and presents a process of investigating attacks against the converged network.

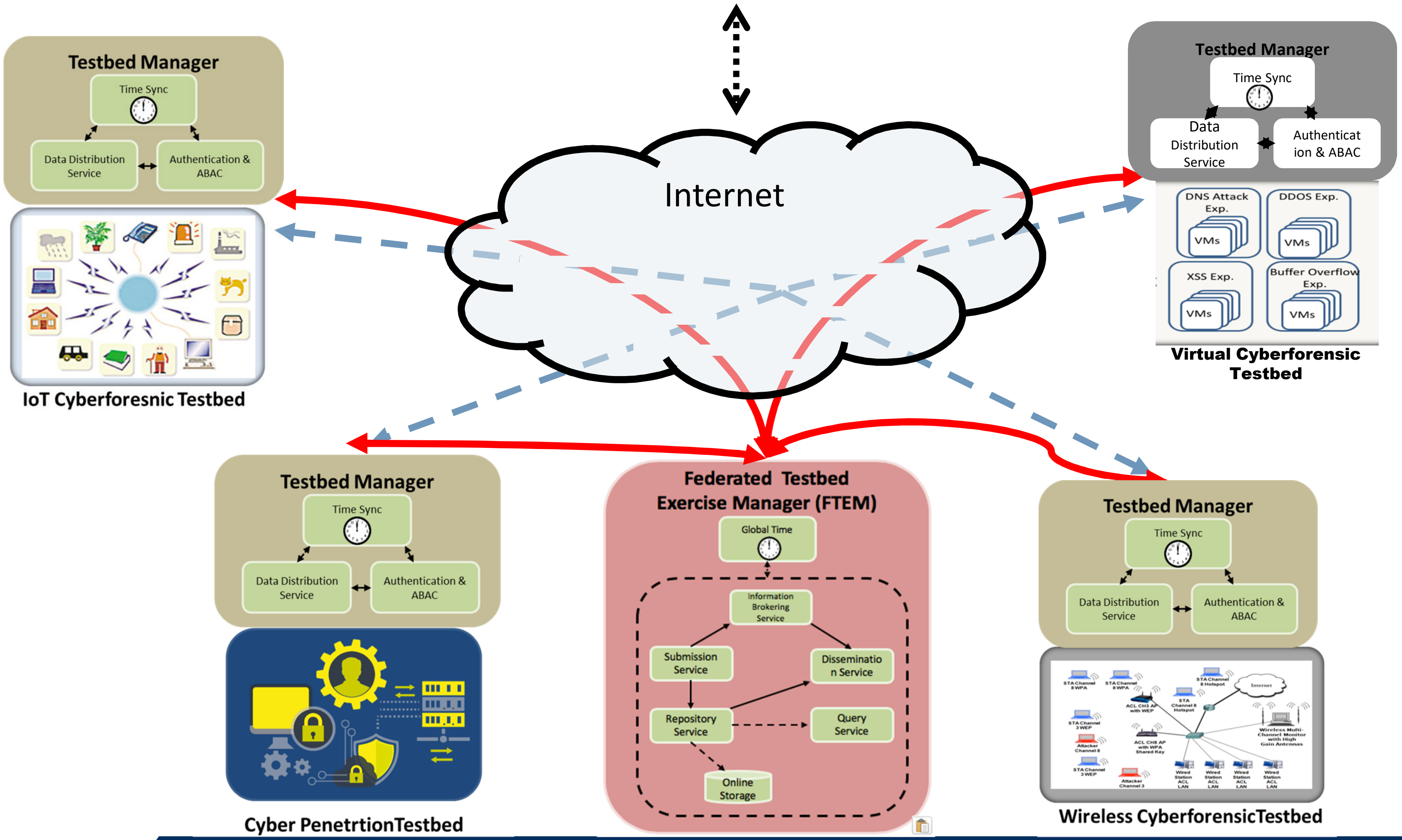
Cloud Evidence Collector



Simplified Cloud Forensic System Architecture



Researchers, and Forensic Investigators

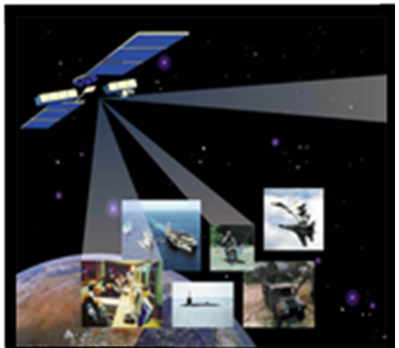


Conclusions

- Implement network forensics as a secure and convenient method of collecting/analyzing digital evidence in UCaaS.
- Patterns can guide systems development, be used to evaluate existing designs, be a basis for simulation, and be a pedagogical tool.
- Approach provides a precise framework where to apply security.
- 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 network forensics.
- Potential to be used as evidence. Forensic patterns value may be realized when semi-formal models are reused on similar investigations.

Moving Forward

- 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



SPAWAR®

Systems Center
PACIFIC