SPAWAR
Systems Center
PACIFIC

Steganophony: Challenges and Detection of Exfiltration Attacks

16 November 2017

Juan C Bennett, Ph.D.

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

SSC PAC MISSION

From concept to capability via…

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

Cyber Forensics Research Lab

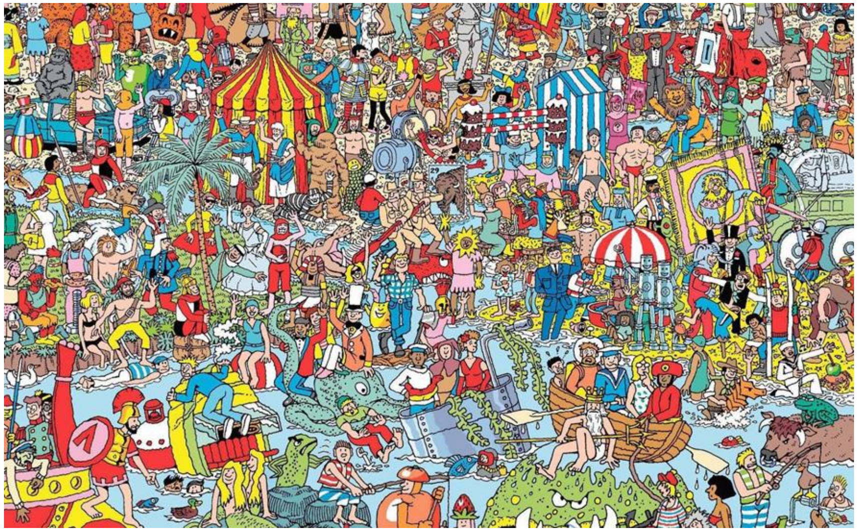
Mission

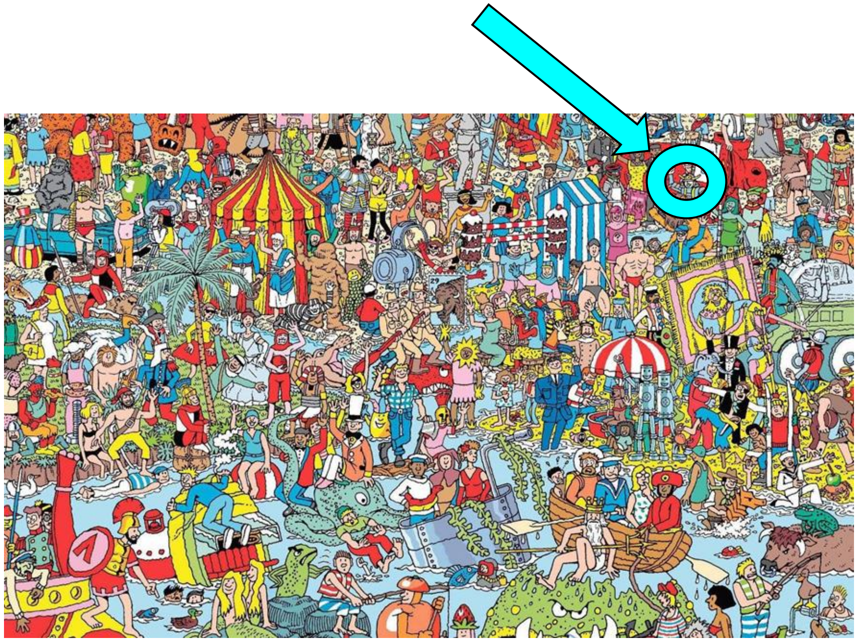
- Investigate novel ways to collect, protect, analyze network-based evidence.
- Understand collection, classification/exploitation of knowledge about adversaries (cyber threat intelligence) from a cyber-forensics perspective.
- Perform network forensics investigations in different DoD environments (e.g.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

Operational Relevance

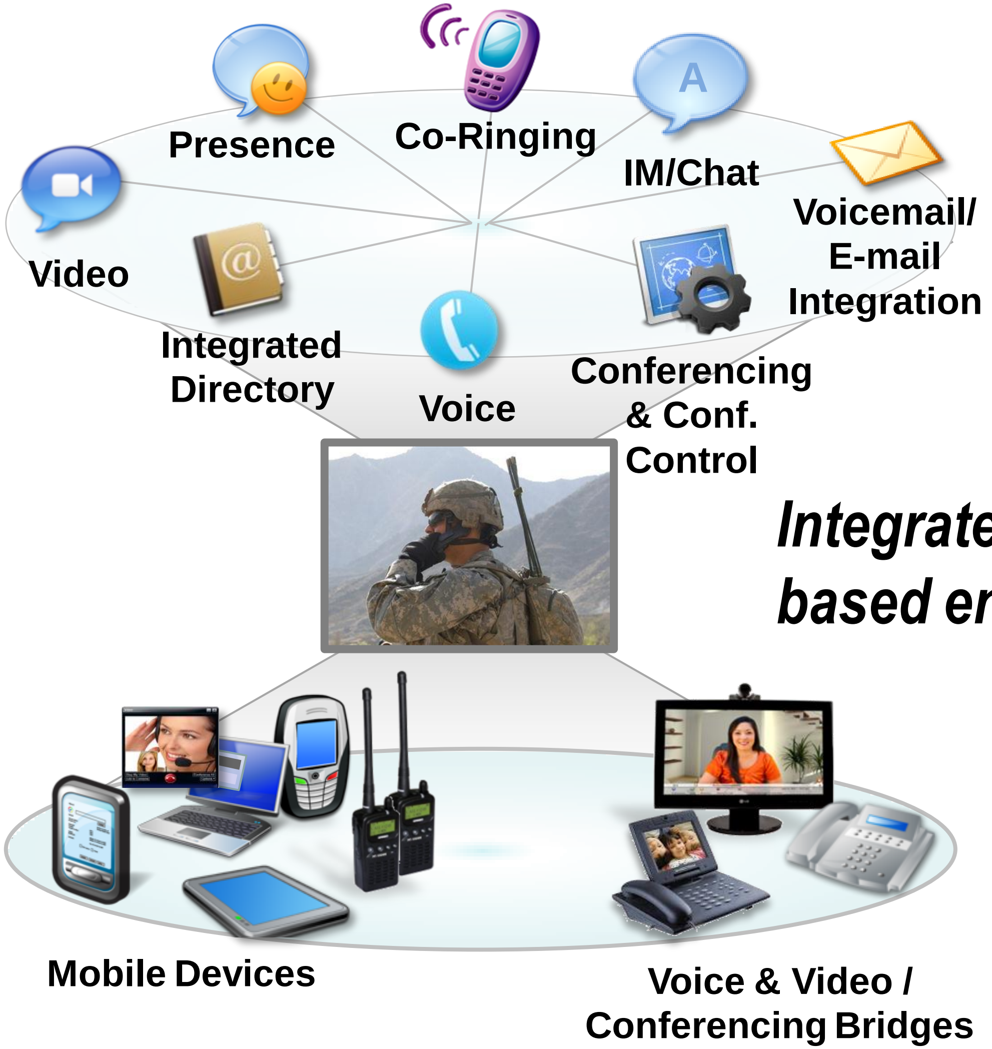
- Enables DCO forces to detect incidents across multiple Navy networks
- Allows DCO forces to conduct network monitoring and analysis within a converged environment
- Develop novel forensic tools and methods to conduct live cyber forensic investigations
- Support network investigators to identify actual 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

Background: What’s Steganography?





Unified Capabilities



Integrated, fully-converged, cloud-based environment

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.

UC Pattern System

- **Architectural patterns**
  - Analyze existing VVoIP architectures in UC**.**
  - Focus on modeling tactical architectures using UML language.
  - 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 the 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 intrusion detection, auditing, and checking points.
  - Help network investigators to select evidence

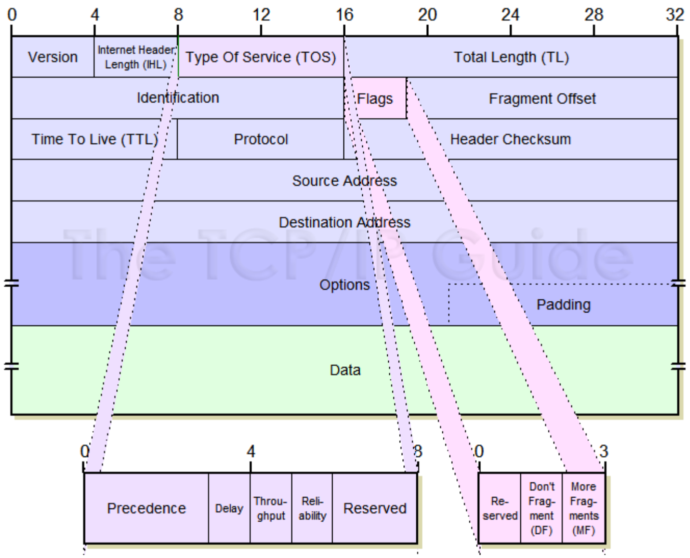
Network Forensics Patterns

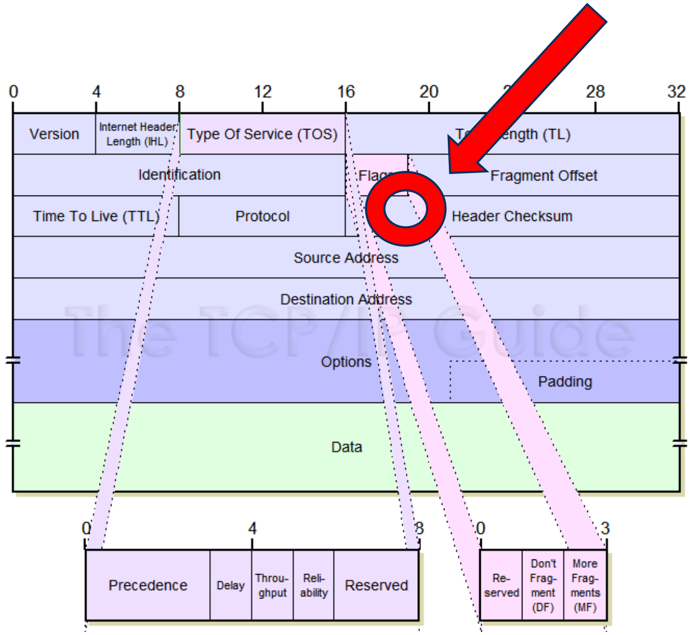
- Extra dimension of protection to the system.
- Abstract view of forensic information to network investigators.
- Enable faster response and more structured investigations of network attacks.
- Discover source of security breaches
- VEC to collect attack packets on the basis of adaptively setting filtering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

Use Case: Signaling Steganophony Pattern

Context

- Subscribers engage in a voice call conversation over a VoIP channel.
- Signaling protocols: H.323 and SIP. Signaling messages are exchanged between endpoints.
- Use of cryptographic protocols (e.g. AS-SIP in TLS, SIPS) which encrypts signaling to improve the security of VoIP connections.





Use Case: An OPSEC Approach

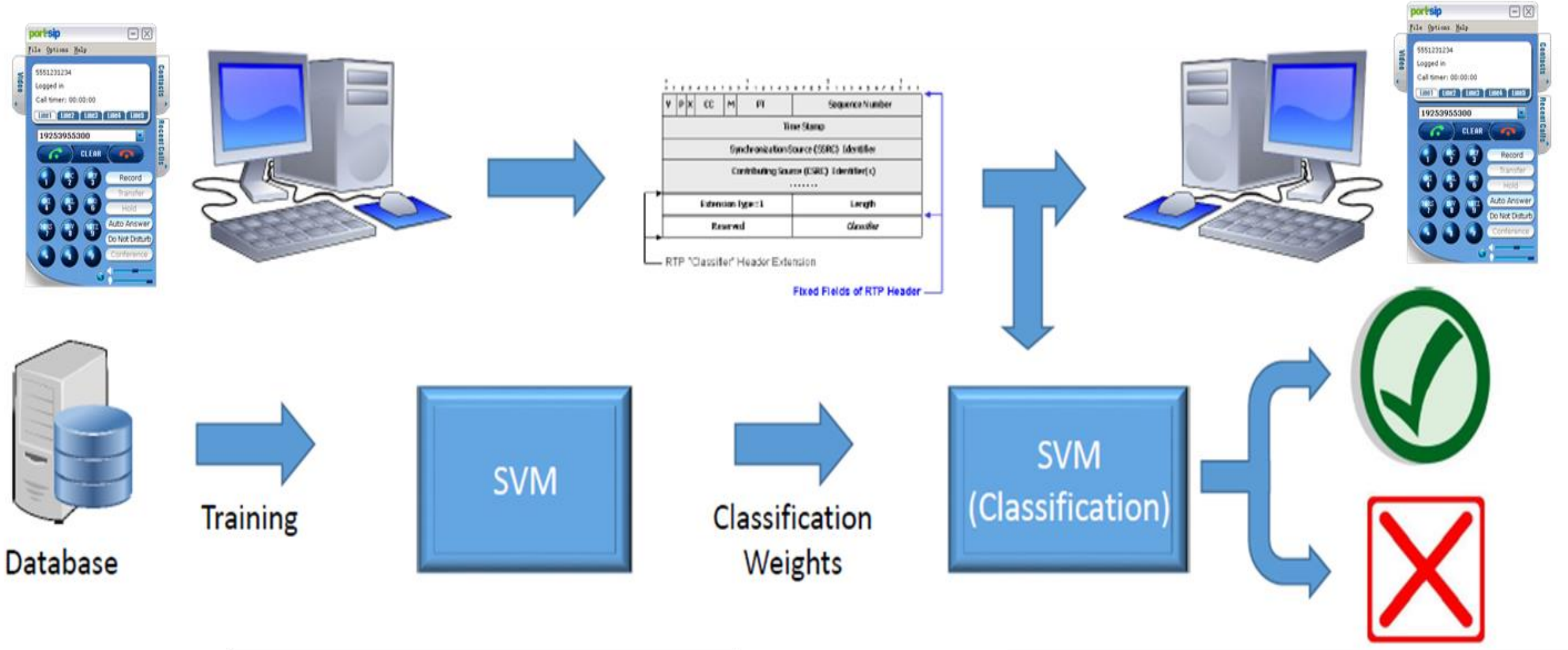
Problem

- How to transmit a secret message to a remote user in a regular conversation via the VoIP system?

Vulnerabilities

- Digital audio signals are, due to their stream-like composition and the high data rate, appropriate covers for a steganographic method
- Creation of covert channels in SIP is possible because in the protocol specifications there are no restrictions to generating parameters about the desired length.
- VoIP connection does not give examiners enough time to detect possible abnormality
- Amount of information that attackers can covertly transfer in VoIP networks is significant.
- Use of steganophony should be considered as a threat to the security of the converged network as it may be used for data exfiltration.

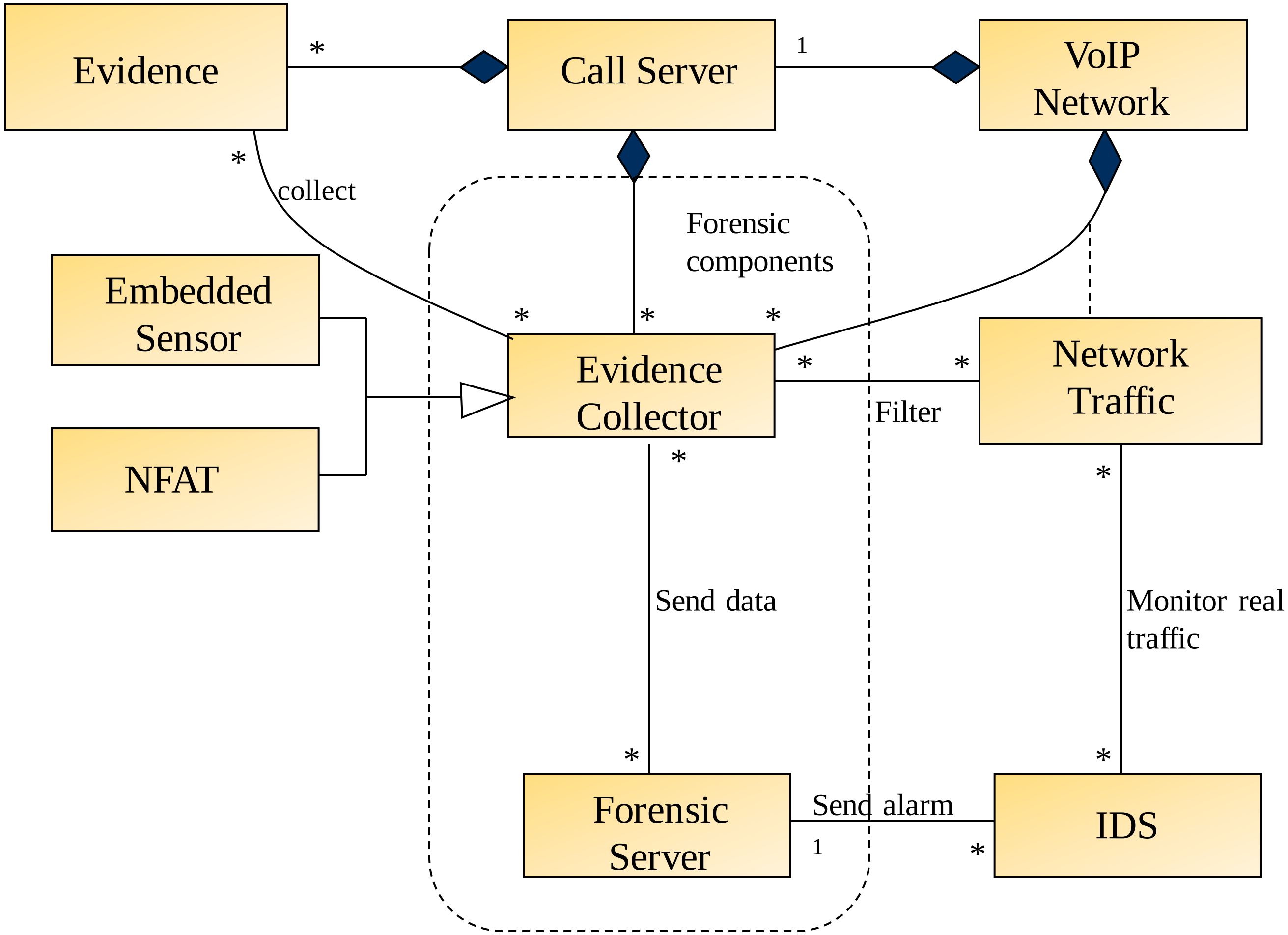
Statistical-based IDS Approach


portsip
V
P
X
CC
M
PT
Sequence Number
Time Stamp
Synchronization Source (SSRC) Identifier
Contributing Source (CSRC) Identifier(s)
Extension Type=1
Length
Reserved
Classifier
RTP "Classifier" Header Extension
Fixed Fields of RTP Header
Database
Training
SVM
Classification
Weights
SVM
(Classification)

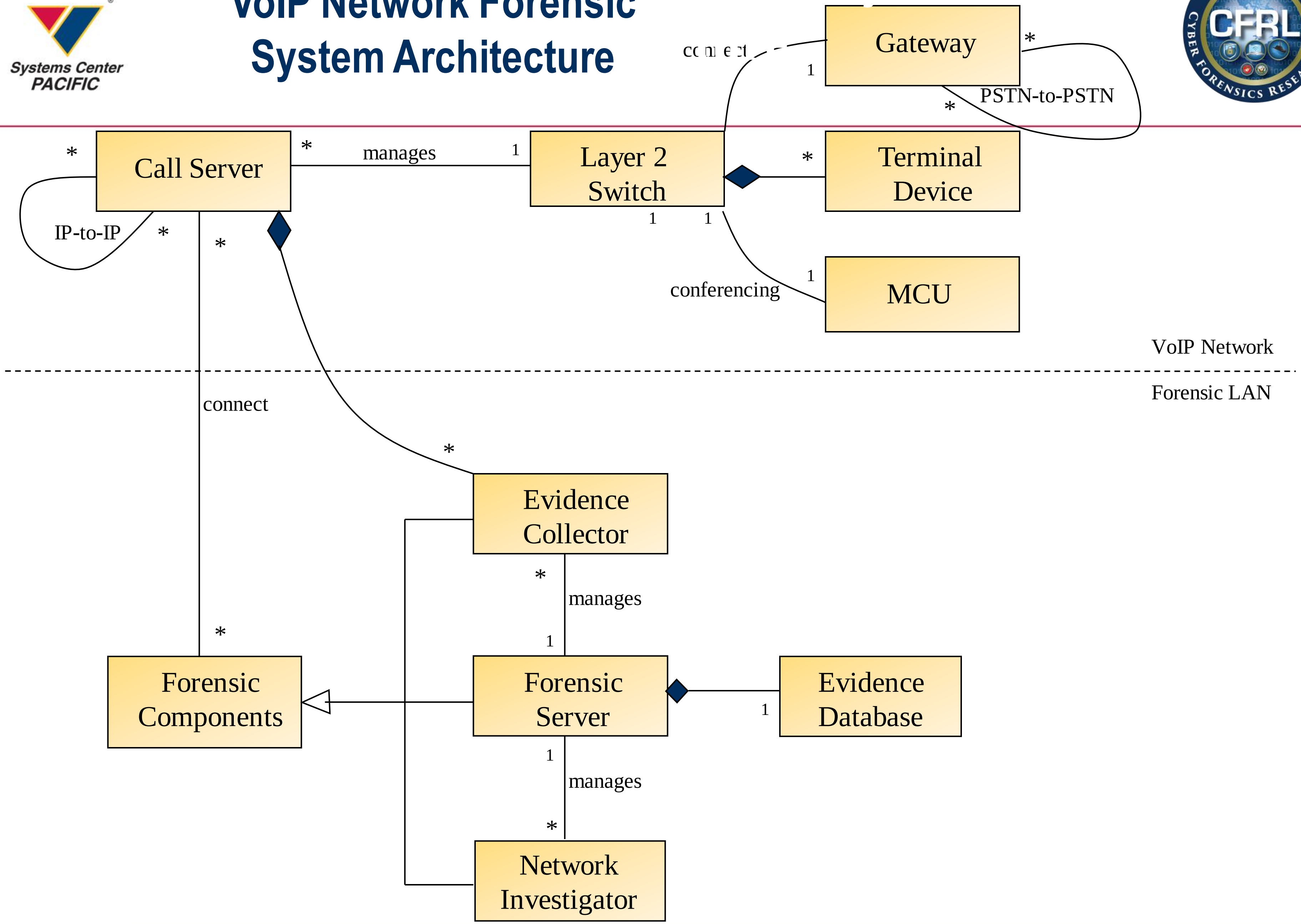
Forensics

- VoIP Evidence Collector pattern to collect attack packets on the basis of adaptively setting filtering rules for real-time collection.
- Sensors with examination capabilities that look at VoIP traffic (i.e. signaling and media) and flag packets where typically unused bits/fields actually have data stored.
- VoIP Evidence Analyzer pattern which analyzes the collected forensic data packets, and presents a process of investigating attacks against the VoIP network.
- Misuse patterns indicate where to look for attack data, which components of the network may be more useful to find evidence, and which parts of the network should have additional capabilities to collect forensic data.

Evidence Collector Class Diagram



VoIP Network Forensic System Architecture



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

Conclusions

- Approach provides a precise framework where to apply security.
- Patterns can guide systems development, be used to evaluate existing designs, be a basis for simulation, and be a pedagogical tool.
- Implement network forensics as a secure and convenient method of collecting/analyzing digital evidence in UC.
- 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

- Strong demand for Cyber security and forensics
- Increasing demand for integrated UC Forensic (UFO)

  Framework, rapid prototyping and experimentation
- Expand misuse pattern catalog (new/evolving attacks)
- Live-forensics vs. post-mortem
- Automated network forensics system (MS&A)
- UC / Cloud forensics

SPAWAR®

Systems Center
PACIFIC