A Model-based Methodology for Developing Secure VoIP Systems

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Juan C Pelaez, Ph. D.

November 24, 2010

VoIP overview

- What is VoIP?
- Why use VoIP?
  - Strong effect on global communications
  - VoIP will replace PSTN soon
  - Voice over IP over Wireless (VoIPoW)
  - Cost savings
  - IP network is used as a backbone between two voice switches/gateways

VoIP on Tactical Networks

- VoIP can traverse radio networks
- US Army is converging on a standard IP backbone in all of the tactical systems (sensor, ISR, UAV or intelligence systems)
- VoIP over tactical networking technology is useful not only to the military, but also to law enforcement and emergency services.
- VoIPoW is becoming available for both wireless LAN and wireless WAN applications.
- U.S. Army is using VoIP on high level units (expecting to be fully implemented soon).
- Disadvantages
  - Security issues
  - QoS issues

Network Architecture Challenges

- Comprehensive understanding of the main issues for both the signaling and the standard protocols used today for providing wireless access in VoIPoW.
- H.323 and SIP protocols for signaling and call control in VoIP, they are essential for providing total access and for supporting IP-based services.
- H.323 is complex and requires a combination of components to perform its functions.
- Need high-level specification of the VoIP architecture that can be used to conduct forensic investigations in a tactical environment.
- Analyze the interoperability with other multimedia service networks and terminals. Terminal devices in disparate networks communicate frequently.

Network Architecture Challenges (Cont)

- Converged environments have a large variety of users and require the use of multiple signaling protocols.
- Examiners usually conduct investigations in architectures that support both SIP and H.323 calls. Therefore our network forensic model must be able to operate in a converged environment using multiple existing and potential signaling protocols.
- Wi-Fi and WiMax are the two standard protocols used today for providing wireless access in VoIPoW.
- Interworking between IEEE 802.11 and IEEE 802.16 is common since the WiMax purpose is to expand the range of wireless systems access.

DFRWS Framework (from [DFRWS01])

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Event/Crime Detection	**Case Management**	**Preservation**	**Preservation**	**Preservation**	Documentation
Resolve Signature	Imaging Technologies	**Approved Methods**	**Traceability**	**Traceability**	Expert Testimony
Profile Detection	**Chain of Custody**	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	**Time Synch.**	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		**Legal Authority**	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	**Link**	
		Data Reduction		Spatial	
		Recovery Techniques			

Network Forensic Challenges
-Collection-

How to efficiently collect digital attack evidence in real time from a variety of VoIP components and networks?

Forces

- Firewalls and Intrusion Detection Systems (IDS), cannot detect or prevent all attacks.
- In Tactical environments we need network models that allow not only the detection of complex attacks, but also that support forensic evidence collection, storage and analysis.
- VoIP, requires an automated collection of forensic data in order to provide data reduction and correlation.
- Need forensic methods with shorter response times because the large volume of irrelevant information and increasingly complex attack strategies make manual analysis impossible in a timely manner.
- In VoIP network forensics a systematic approach is needed to detect vulnerabilities and the resulting attacks.

Network Forensic Challenges –Analysis-

How to analyze evidence in order to discover the attack source and other characteristics of the attack?

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.
- Wireless anti-forensics methods
  - The modification of the 802.11 specification (Raw Covert, madWifi patches)
  - Use of illegal channels
- The forensic analysis process must guarantee data preservation and integrity.
- Attacks in converged networks are becoming more frequent and more complex to counter.
- Need to reusing network forensic knowledge and documenting forensic investigations.
- Lack of experience executing investigations or using similar forensic tools.

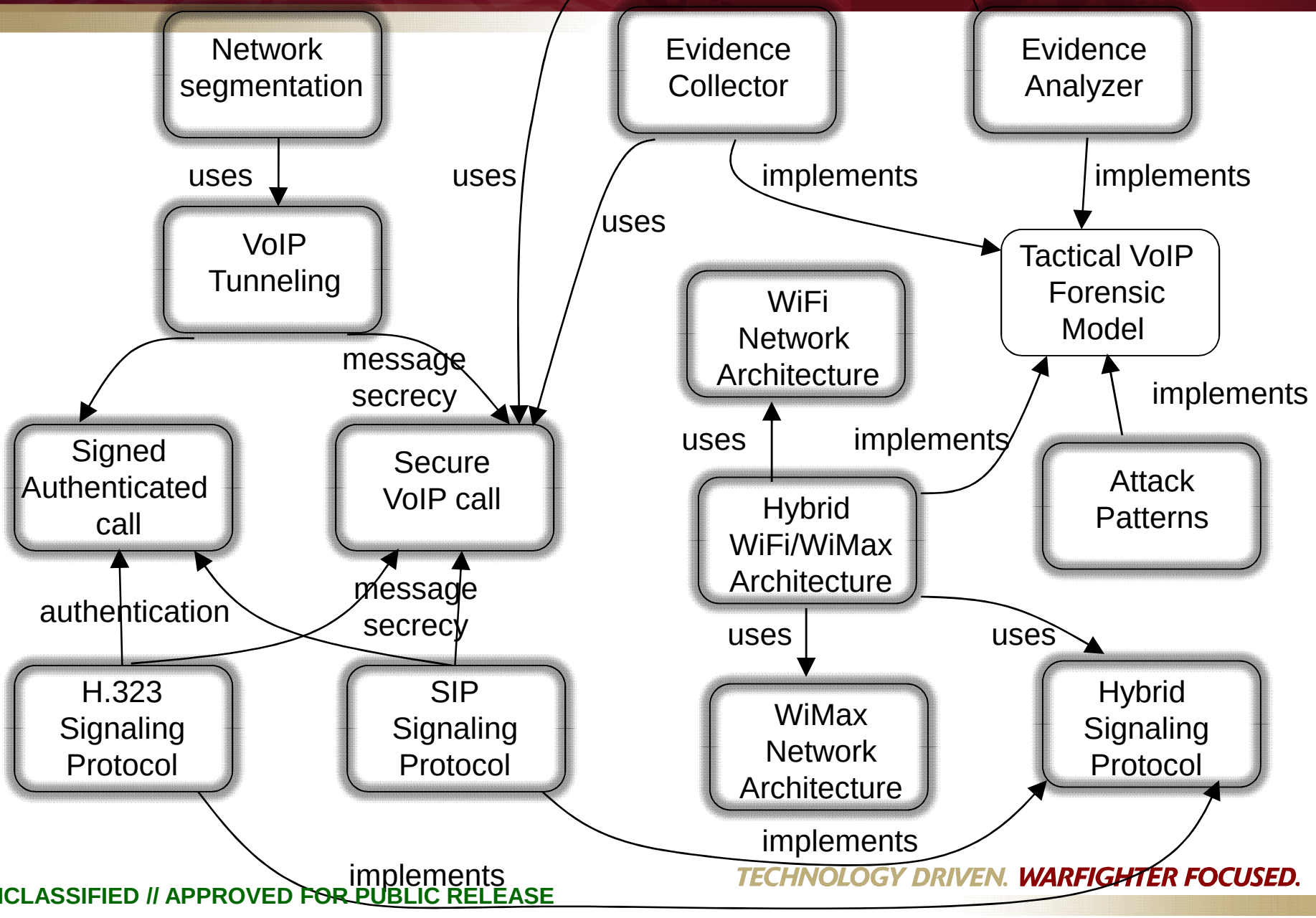
Network Models using Patterns

- Study VoIP network representations to model, simulate, test, and prototype networks with intent to discover new ways to characterize network environments and the information embedded in the network.
- A comprehensive pattern system based on a collection of architectural, attack, forensic and security patterns, providing best practices for IP telephony systems.
- Analyze network forensic investigations in a VoIP converged environment using the existing methods for this basis.
- A pattern system to specify, analyze and implement network forensics investigations for different architectures. We will make use of UML (Unified Modeling Language) to describe these patterns.
- Effective ways for network investigators to implement the use of network forensics as a secure and convenient method of collecting digital evidence in a VoIP environment.

VoIP Pattern System

- **Architectural patterns**
  - Analyze existing VoIP architectures in IP telephony**.**
  - Focus on modeling tactical architectures using UML language.
  - Patterns are used for high-level specification of the VoIP system.
- **Attack patterns**
  - Systematic description of the steps and goals of an attack and ways to defend and trace its application in a system.
  - Attack pattern template in order to describe how to document and organize generic attack patterns.
  - Attack pattern catalog.
- **Security patterns**
  - Based on security mechanisms and standards to stop attacks against the VoIP system.
  - From the list of attacks we can figure out what security patterns are necessary to prevent or mitigate the threats.
- **Forensic patterns**
  - Capturing, recording, and analyzing information collected on VoIP networks from several intrusion detection, auditing, and checking points.
  - Help network investigators to understand which evidence can be obtained from the VoIP system after a specific attack.

VoIP Pattern System



Example: Signaling Steganophony Pattern

Defines a structure and process to manipulate signaling protocol information in converged networks for steganographic purposes. Provides a way to exploit unused fields in signaling packets to embed hidden messages in VoIP calls.

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. SIPS) which encrypts signaling to improve the security of VoIP connections.

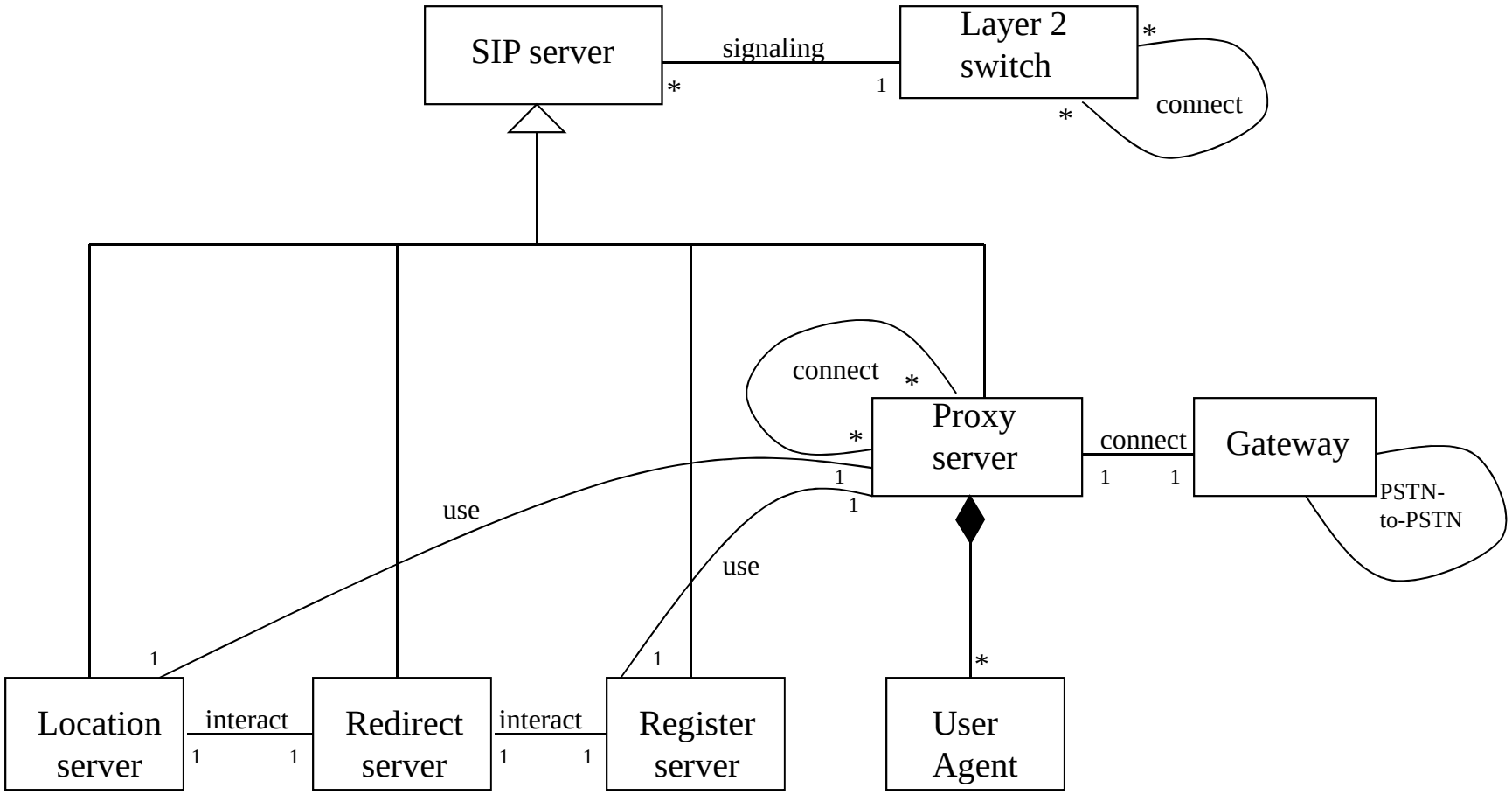
Problem

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

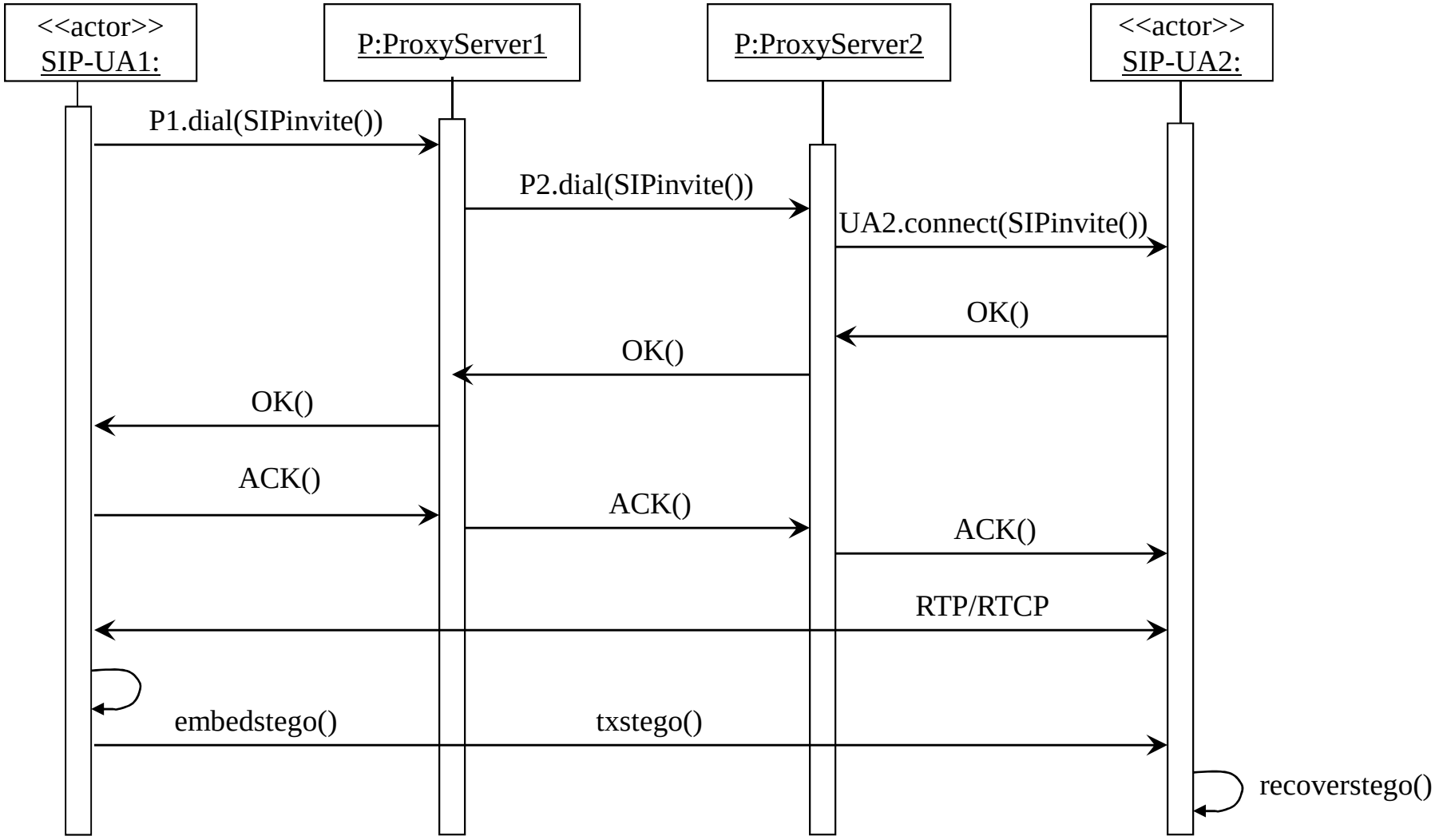
Vulnerabilities

- 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.
- A 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.
- The use of VoIP steganography should be considered as a threat to the security of the converged network as it may be used for data exfiltration.

Class diagram for a SIP architecture



Sequence diagram for SIP signaling steganography



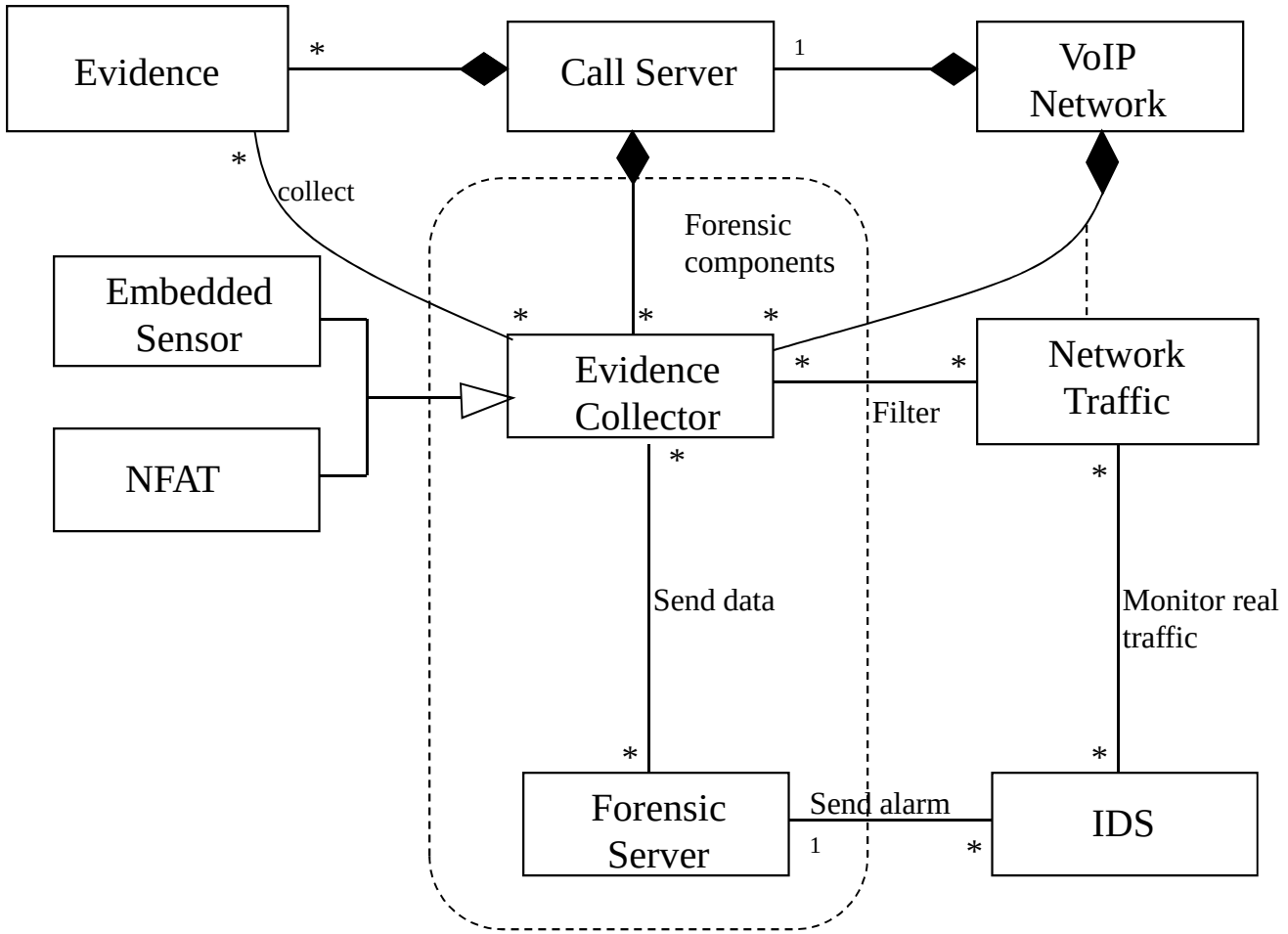
Countermeasures

- Use statistical analysis of the lost packets for calls in the converged network by observing RTP streams flow this may indicate potential use of VoIP steganography.
- Use the Network Segmentation pattern which performs separation of the voice and data services to improve data exfiltration detection in VoIP.
- Analyze the voice packet payload in order to decide whether it contains voice data consistent with the overall call or not.
- Use Stateful-Inspection Firewalls or Session Border Controllers with Deep Packet Inspection (DPI) technology in order to detect hidden messages in VoIP. DPI looks inside the voice packet, and analyze the contents of the packet as well as the headers to decide if the information contain steganographic data or not.

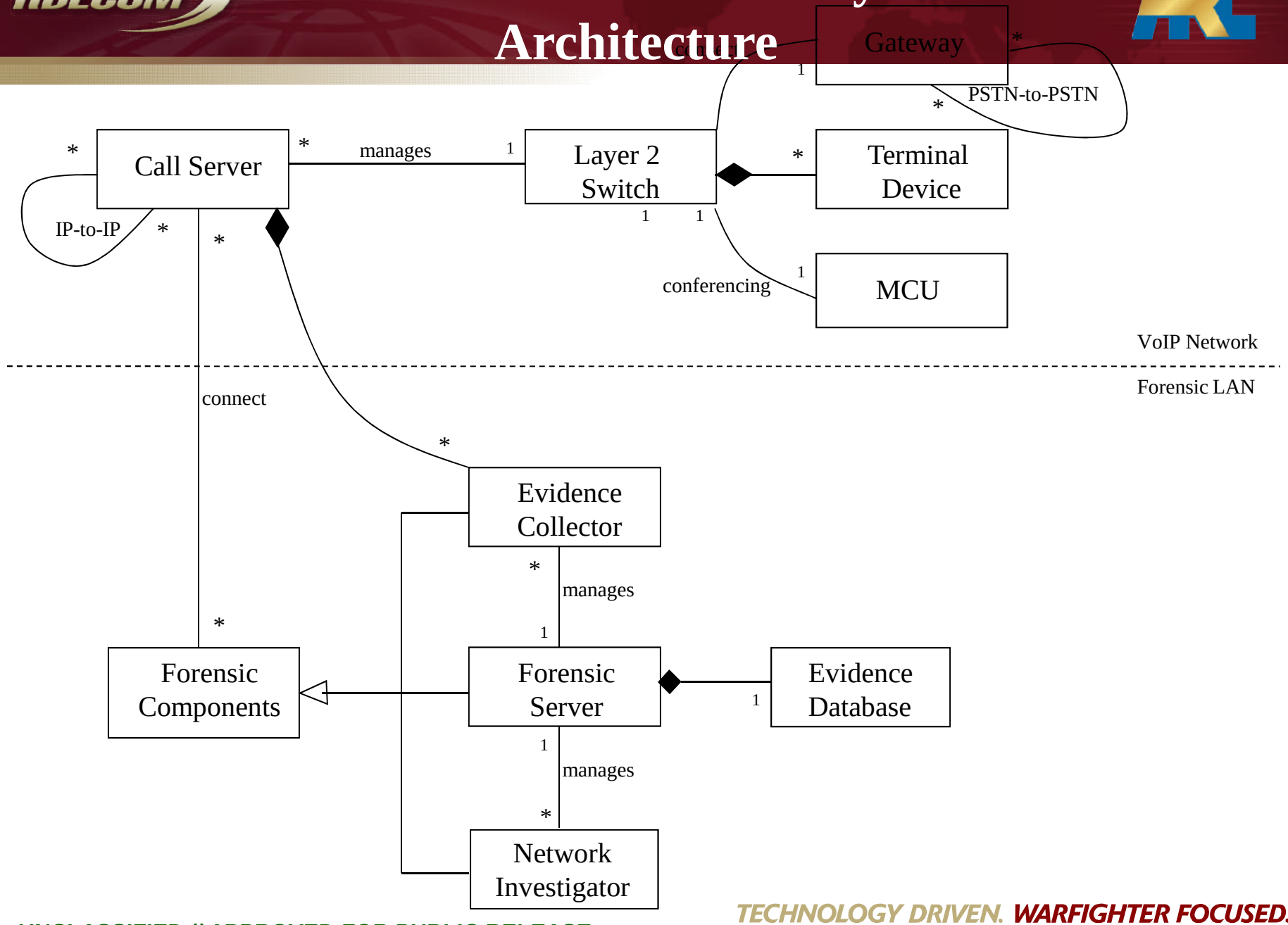
Forensics

- Use the VoIP Evidence Collector pattern which defines a structure and process to collect attack packets on the basis of adaptively setting filtering rules for real-time collection.
- Use 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 in them.
- Use the VoIP Evidence Analyzer pattern which analyzes the collected forensic data packets, and presents a process of investigating attacks against the VoIP network. This pattern may also use steganalysis algorithms to analyze VoIP steganographic attacks.
- 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



Conclusions and Future work

- VoIP will become more typical in the near future, with the probability of being the most popular system for mobile communication, therefore, it is important to study the mechanisms and tools for forensic analysis of converged networks.
- Forensic information found in VoIP systems has a great potential to be used as evidence. Forensic patterns value may be realized when semi-formal UML models are reused on similar investigations.
- This research presented effective ways in which network investigators can more effectively implement the use of network forensics as a secure and convenient method of collecting and analyzing digital evidence in a VoIP environment.
- A contribution in this research is the creation of a comprehensive pattern system to be used in forensic investigation processes.
- We concentrated on the functionality offered by these patterns and their usefulness. These are the first steps toward a methodology for modeling network forensics.
- Generation of additional forensic patterns including IDS versions of this approach. Explore statistical approaches for IDS in converged environments