An Architecture for Security Auditing in Converged Networks

• ***Dr. Abdur Rahim Choudhary*** •
arc@lucent.com, 410-309-7025

Lucent Technologies
Bell Labs Innovations

And

• *Presented to*•
University of Maryland Institute of Advanced Computer Studies (UMIACS)

May 01, 2003

Disclaimer

The views expressed in this talk are my own, and do not represent the views of my employer (Lucent) or my customer (LTS) or my co- investigators

Outline

- Background
  - LTS research project
  - Industry landscape
  - What is security auditing
- Dual-use approach to Security Auditing
- A possible role for UMIACS like forums
- An architecture for security auditing in converged networks
- Conclusions

LTS Project

- Participants: Telcordia, Lucent, LTS
- People: Jeff Friedhoffer, Gary Hayward, Bob Horgan, Rahim Choudhary, and many others.
- History:
  - Phases 1 and 2 completed, started early 2001.
  - Phase 3 to complete September 2003.
  - Phase 3 has a substantial ‘prototyping’ component.

Industry Landscape

- 'Popular Expectation' is that VoIP will 'Take Off'
  - How do we do familiar functions in VoIP: e.g. GETS and CALEA
- 'Expectation' is that 'Advanced' services will be enabled by VoIP
  - How do we monitor/audit these services, including the VoIP itself, for
    - 'security events' and for
    - a generalized version of GETS and CALEA like functions
- Security is expected, but willingness to pay for it is not obvious in the industry and the commercial world.
  - Would a commercial customer pay extra for a product because it is more secure?
  - Need to provide security capabilities without additional costs
  - Hence DUAL-USE of existing data to develop new security capabilities
    - OAM&P data
    - QoS data

What is security auditing?

- Security auditing means to examine data for events that are of interest from a security point of view. These events are analyzed using rules that an organization adopts for its security operations.
  - The rules that represent an organization's security point of view and the corresponding operations comprise the organization's 'security policy'.
  - Auditing without a 'security policy' is meaningless.
- What data should be examined for security auditing?
  - Depends on the objectives of the security audit.
  - OAM&P data are an obvious candidate, other than the security audit specific data if available.

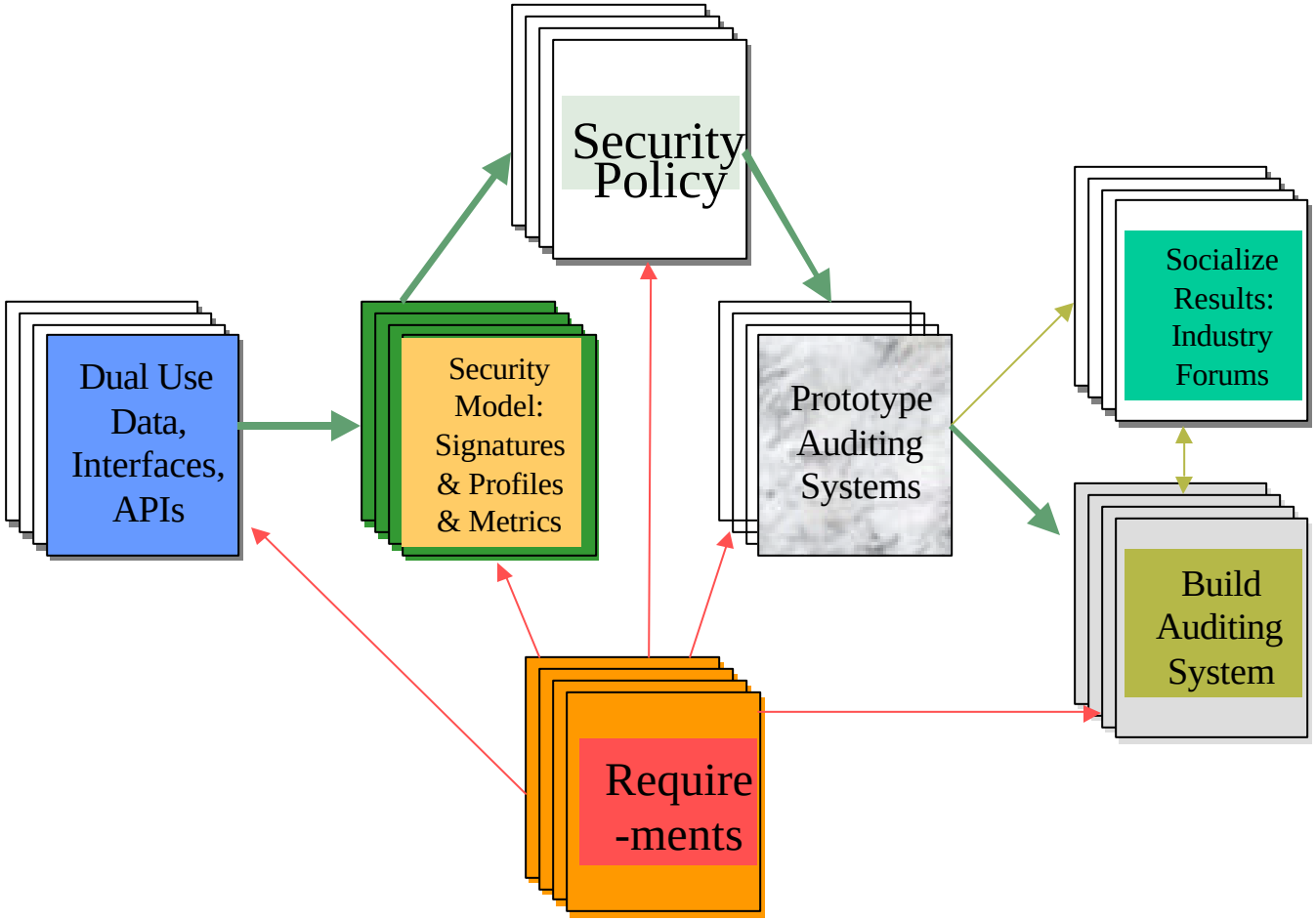
Approach: Get Dual-Use Information

- Identify dual-use information from the OAM&P activities
  - Some data that our research analyzed are the following.
    - Call detail records (CDR), basic, supplementary, and third party
    - Alarms sent by systems, subsystems, and applications
    - Logs generated by the systems, subsystems, and applications
    - Information in databases, e.g. services/subscriber database
  - Some data that we could analyze but did not
    - Information in the MIBs and PIBs
    - QoS related information, e.g. RAQMON work at IETF under Remote Network Monitoring working group
- Our research also analyzed
  - the interfaces to extract the dual-use information.
  - APIs to develop security auditing applications.
- Research results are documented in project reports for Phases 1 and 2.

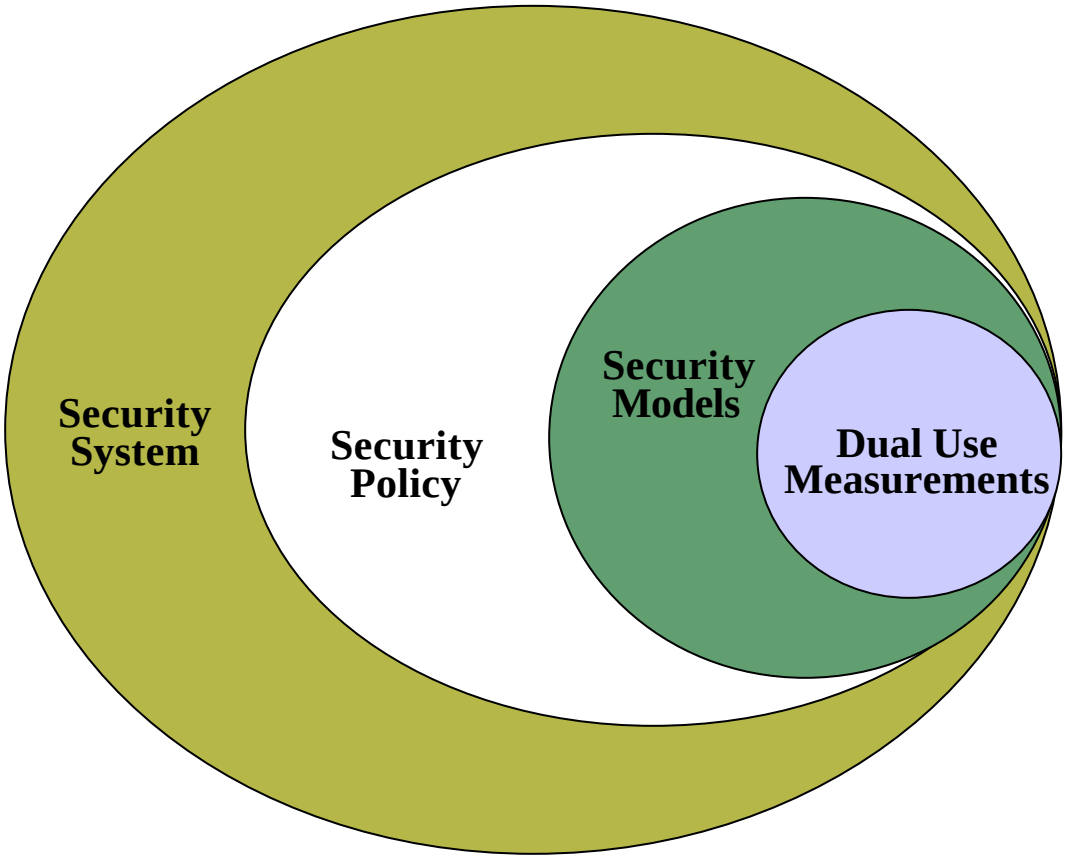
Approach: Dynamic Sensors

- Use the collected dual-use information to define ‘dynamic sensors’
  - “Dynamic Sensors” are programs to detect violations of security policy
    - They can use signatures, profiles, statistical techniques, AI techniques, AI Agents, Fuzzy logic, Pattern Recognition, etc.
      - i.e truly interdisciplinary area perhaps suitable for UMIACS type forum.
    - Problem of false positives and false negatives.
      - i.e truly interdisciplinary area perhaps suitable for UMIACS type forum.
  - They can detect “potential” violations ***before*** they happen.
    - The dynamic sensors not only detect the “violations” of an organization’s security policy, but they can also detect the “tell tale” signs that are precursors for such violations.
      - **A challenge to UMIACS type forums**.
      - Problem can not admit a global solution

Approach: Schematics



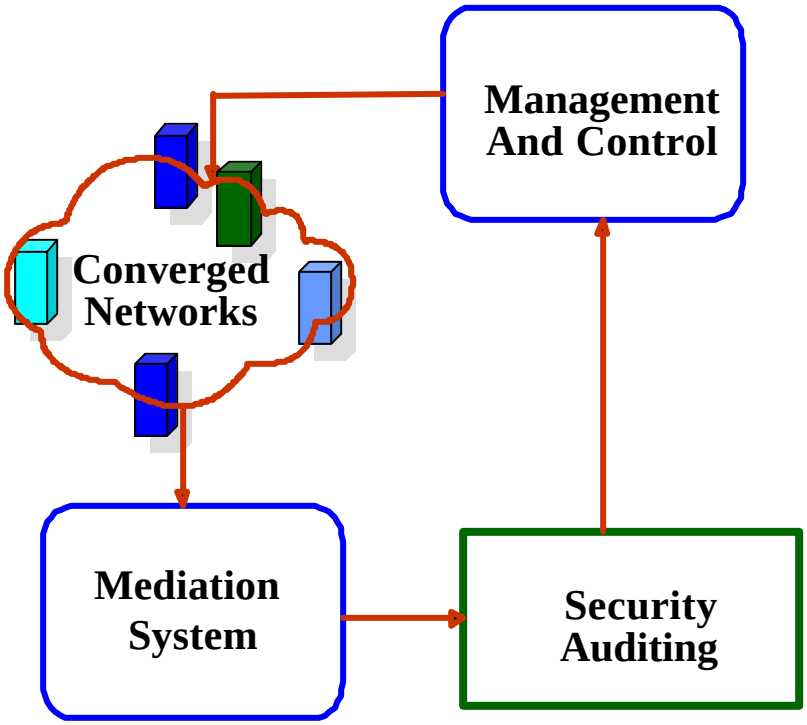
Approach: Building Blocks



An Architecture

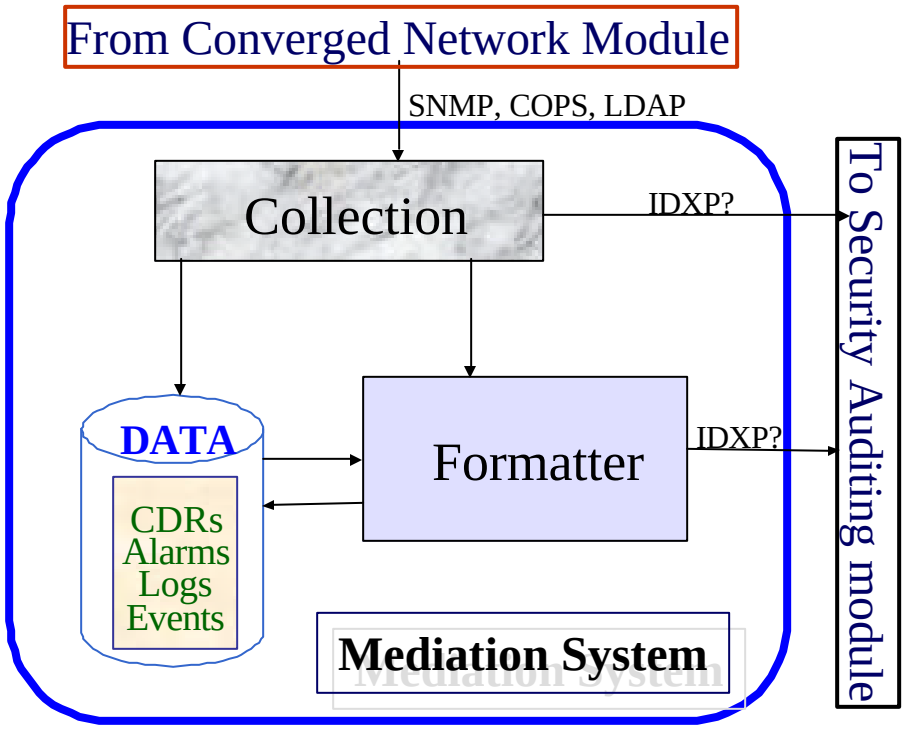
- We need an architecture to integrate these research components, so that a security auditing system can be built out of them.
- Some of the requirements for such an architecture are clear. Based on the needs of the organization performing the security audit, the architecture must allow for
  - Collection of the ‘needed’ dual-use information.
  - Various ‘levels’ of sophistication in the analysis on the dual-use data.
  - ‘Multiple Levels’ of complexity in security policies.
  - Respond to the prediction and/or detection of a security policy violation.
    - Manually through a human operator
    - Automatically by well tested and intelligent software
  - Prioritization of services and events.

An Architecture: High Level



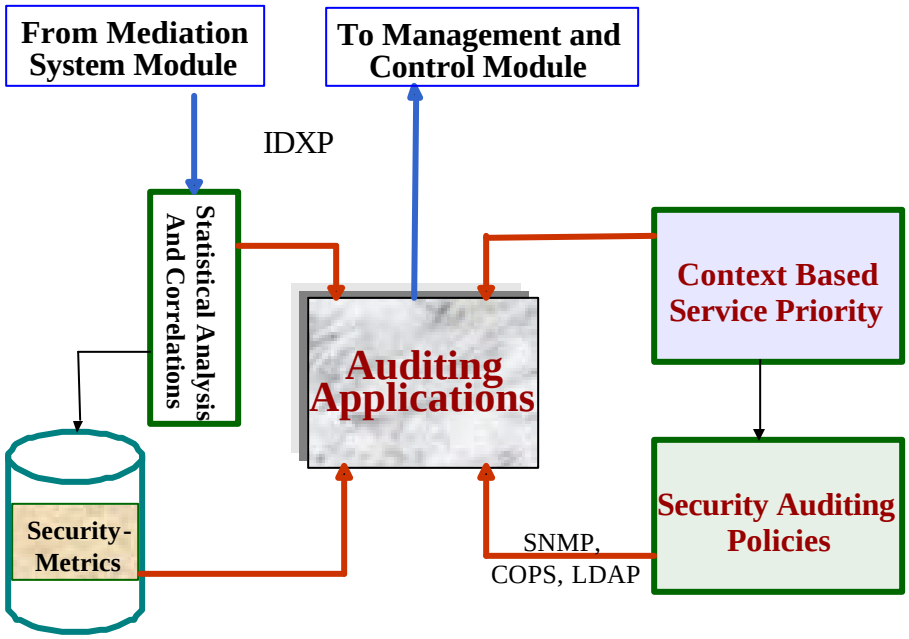
- Mediation system negotiates with the network elements, or their proxies, to collect the needed dual-use data.
  - Understands the network
- Security Auditing module performs the analysis, implements multiple levels of security policies, carries out prioritization, and decides the desired response(s) to the violations.
  - Agnostic of the network
- Management and Control module translates the responses to the violations to the network specific commands.
  - Understands the network
  - A proxy to OAM&P system

Module: Mediation System



- The collection subsystem is where the network knowledge residues.
  - SNMP, COPS, LDAP
  - Organization determines what dual-use data it needs.
- The formatter subsystem converts the data into a canonical form.
  - A third party Security Auditing module should understand the data.
  - The IDWG work at IETF on IDXP: The Intrusion Detection Exchange Protocol.
- The data storage subsystem archives the CDRs, Logs, Alarms, and other Events.
  - Retrieval per request by the Security Auditing module.

Module: Security Auditing

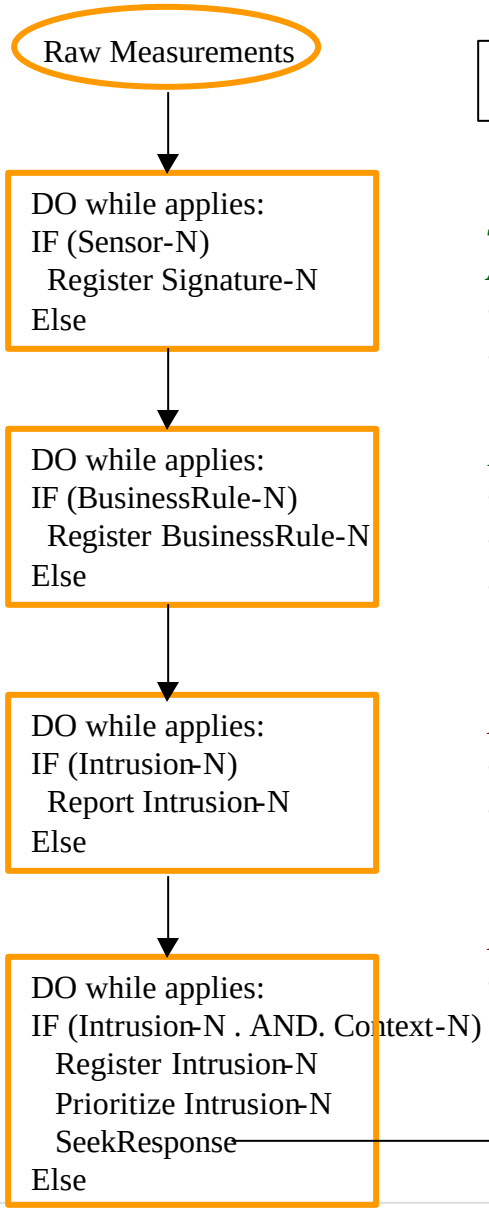


- Auditing applications subsystem provides a security auditing service.
  - Detailed architecture provided.
- Statistical analysis and correlations module supports the analysis of the dual-use data to the desired level of sophistication.
  - Some results of this analysis are generated in the form of “Security-Metrics”.
  - Organization decides what security metrics it needs.
- Next page describes the two modules:
  - Security Auditing Policies and
  - Context Based Service Priority

Security Auditing Module: Policies

- Security Auditing Policies subsystem allows an organization to specify its auditing objectives and operations.
- An organization can need the following policies.
  - Violation Prediction policies
  - Violation Detection policies
  - False positive policies
  - False negative policies
  - Response policies
  - Response prioritization policies
  - Event prioritization policies
- Policies can comprise of the static sensors and dynamic sensors.
- Available standards include SNMP, COPS, LDAP
  - Policy Framework working group http://www.ietf.org/html.charters/policy-charter.html
  - IP Security Policy working group http://www.ietf.org/html.charters/ipsp-charter.html

Policies for Detection/Prediction



A Defense-in-Depth Type Approach

Sensors embody the knowledge and policies about Assets, Threats, and Vulnerabilities

- Assets: What do you want to protect?
- Threats & Vulnerabilities: What do you want to protect it against?

Business Rules define policies on cost/benefit tradeoffs

- Risk Analysis: What is your Mitigation strategy?
- How much risk is acceptable?
- False positive and false negative tradeoffs

Policies on what constitutes an intrusion for your organization

- Know your Adversary?
- Cost of a misjudgment

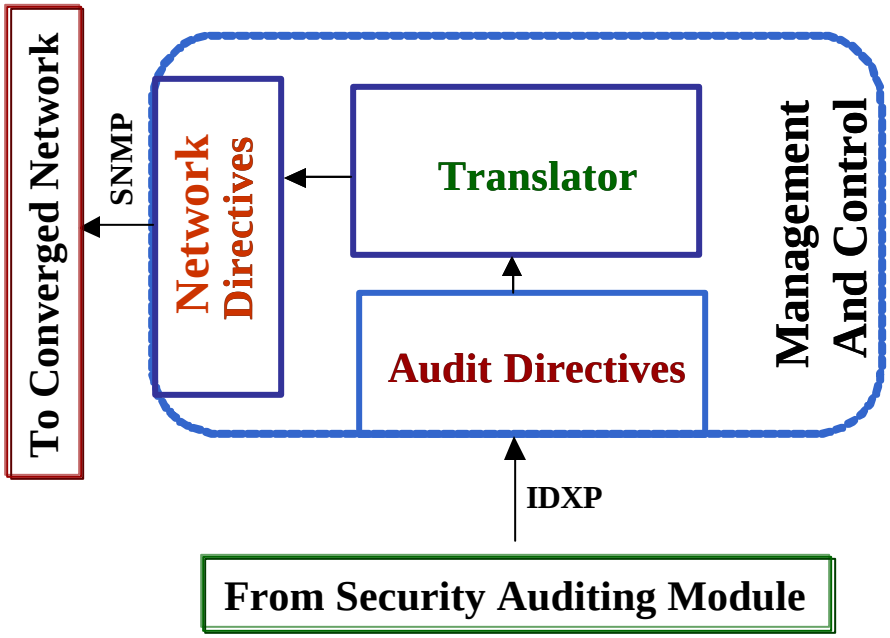
Policies for context based prioritization

- Acquire and use all applicable information

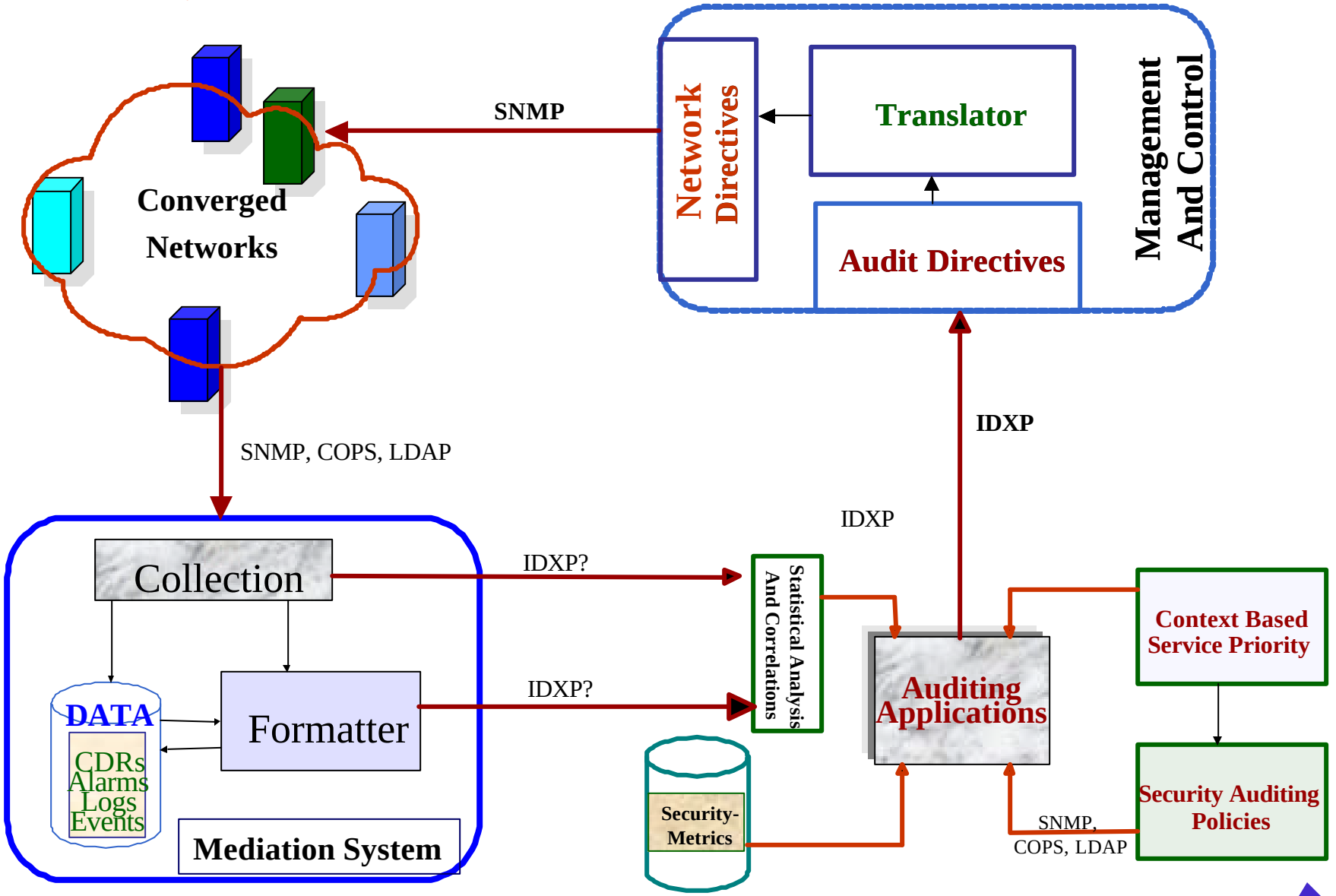
Security Auditing Module: Prioritization

- Context based service prioritization (CBSP) is a concept that we have developed during our research. It embodies three components: the Context, the context based Priority, and the context based Policies.
  - Prioritization of events and response actions is a practical need. A human operator can provision only a finite number of services in a given time.
  - Context information is vital in decision making, especially to handle special situations
- CBSP is used in the following ways.
  - As a mechanism to prioritize events and actions.
    - Severity of an intrusion (Severity classification)
    - Urgency of an action needed in response to an intrusion
  - As an input element for the policy
    - An input parameter to decide whether an intrusion has taken place, or is likely.
    - An input parameter to decide a response to an intrusion.
  - As a mechanism to handle exceptions to the general policy rules
    - To handle special cases, e.g. hot numbers.
    - Handle all traffic ‘normally’ except the CALEA traffic
    - Drop all traffic except the GETS traffic.

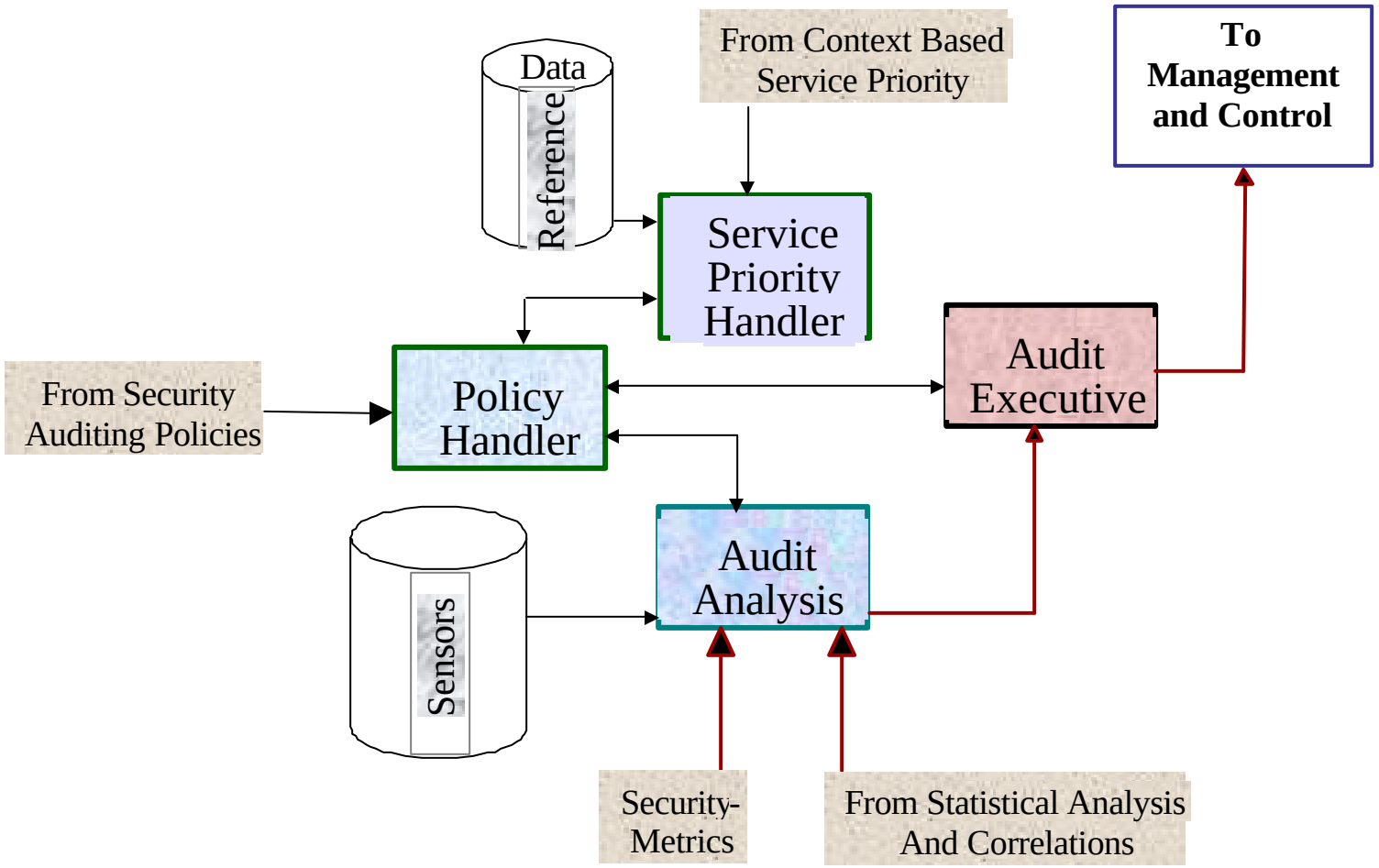
Module: Management and Control



- Interprets the directives received from the Security Auditing module.
- Translates the received directives into OAM&P directives for the network elements.
- Delivers the OAM&P commands to the desired network elements through
  - The relevant OAM&P subsystem
  - The operator console
- The standard interfaces are
  - IDXP with the Security Auditing module.
  - SNMP with the network.

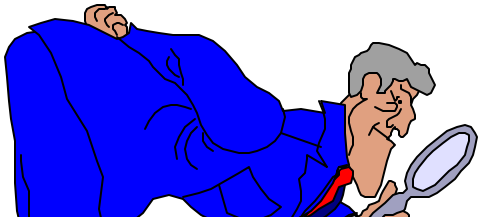

Converged
Networks
SNMP
Network
Directives
Translator
Audit Directives
Management
And Control
SNMP, COPS, LDAP
IDXP
IDXP
Collection
IDXP?
Statistical Analysis
And Correlations
Auditing
Applications
Context Based
Service Priority
DATA
CDRs
Alarms
Logs
Events
Formatter
IDXP?
Security-
Metrics
Security Auditing
Policies
SNMP,
COPS, LDAP
Mediation System

Security Application

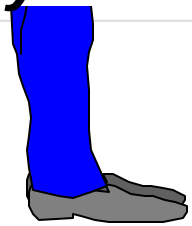


Security Application (cont)

- Audit Analysis subsystem decides if a violation is predicted or has occurred. It uses the following input.
  - The results from the Analysis and Correlation module,
  - The “Security Metrics”
  - Violation “Sensors”
  - Various policies, as obtained via the “Policy Handler” subsystem
- Audit Executive makes the final decision with respect to the following.
  - The severity of the violation
  - The response action to be taken
  - The urgency of the response action
- Audit executive sends its decision to the Management and Control module. It uses the following information in making the decisions.
  - Decisions from the Audit Analysis subsystem
  - The context based priority, as obtained via the Service Priority Handler subsystem
- The Service Priority Handler determines the priority using the following information
  - A reference database that contains the context information,
  - The relative priorities as obtained via the Context Based Service Priority subsystem
  - Priority handling policies as obtained via the Policy Handler subsystem



Key Findings



- Dual-Use approach to Security
- An architecture to develop Security Applications
  - New Concept: Context based service priority
  - Standards based