
Intrusion Detection

ISA 774
George Mason University
Spring 2006

Technical Issues

GMU ISA 774 Spring 2006 2

Technical Issues for IDS

- Scalability
- Management
- Reliability
- Analysis Issues
- Interoperability
- Integration
- User Interfaces

GMU ISA 774 Spring 2006 3

Scalability

- Scaling over Time
- Scaling over Space
 - How did GrIDS approach the scalability issue?

GMU ISA 774 Spring 2006 4

Management

- Network Management
 - Network management tools can be useful for ID, but are seldom used
 - Why??
- Sensor Control
 - Centralized
 - Decentralized
- Investigative Support
 - Systems are not designed for easy extraction of data for investigation
 - Need to include mechanisms to prove authenticity for legal purposes
 - Does this hinder the other goals of the IDS?
- Performance Loads

GMU ISA 774 Spring 2006

5

Reliability

- Reliability of Information Sources
- Reliability of Analysis Engines
- Reliability of Response Mechanisms
- Reliability of Communications Links

GMU ISA 774 Spring 2006

6

Analysis Issues

- Training Sets for AI-Based Detectors
 - Must have authentic complexity
 - Must be attack free
 - Should be generic
- False Positives/Negatives in Anomaly Detection
 - Need high detection rate and low false alarm rate to be effected and trusted by users

GMU ISA 774 Spring 2006

7

Analysis Issues

- Trend Analysis
 - IDS should be able to discern whole categories of attacks, not just the one instance it knows about
 - See *Automatic Generation and Analysis of NIDS Attacks*
- Composition of Policies
 - Need provable models for high security environments
 - “Cascade vulnerability” or “composability” problems
 - Automated tools to build IDS policies

GMU ISA 774 Spring 2006

8

Interoperability

- Robust, modern IDS requires input from a variety of sources
- Multiple data formats may impact useability
- Two ways to implement interoperability are Standards and Middleware
 - CIDE/CRISIS Effort
 - Audit Trail Standards

GMU ISA 774 Spring 2006

9

Integration

- A counterpart if Interoperability
- IDS needs to be able to work in heterogeneous environments
- IDS needs to be able to be built on top of legacy systems without facilities for robust auditing
 - Process Control and SCADA systems
- IDS needs to work in environments where multiple protocols may be present
 - Process Control and SCADA systems !!

GMU ISA 774 Spring 2006

10

User Interfaces

- Interface design is a major consideration for any system – IDS is no different
- Has the greatest effect on usability
- IDS interfaces present a special challenge due to the large amounts of complex data that must be communicated

GMU ISA 774 Spring 2006

11

8. The Real World Challenge

GMU ISA 774 Spring 2006

12

Roots of Security Problems

- Problems in Design and Development
- RISOS (mid 1970's) project identified major causes of security problems in software:
 - Incomplete/Inconsistent Parameter Validation
 - Implicit sharing of Privileged data
 - Asynchronous validation/inadequate serialization
 - Timing Windows
 - Race Conditions
 - Inadequate identification
 - Violable prohibition/limit (buffer overflow)
 - Exploitable logic errors

GMU ISA 774 Spring 2006

13

Stack Smashing

- Interacting with vulnerable programs
- It is very time consuming and difficult to architect new hacks, and few people can do it (or more importantly, can spend the time to do it)
- Traditional solutions still apply

GMU ISA 774 Spring 2006

14

Problems in Management

- Absence of Security Management Infrastructure
- Failure to Ship/Correct Default System Configurations
- Failure to Coordinate Components of Protection Scheme
- Failure to Train Personnel Properly
- Human Error

GMU ISA 774 Spring 2006

15

Problems in Trust

- Roots of Trust Issues
- Personnel Trust and Security Perimeters
- Network Interhost Trust Issues
- Protocols and Trust Issues
 - Major Internet protocols are all “legacy”

GMU ISA 774 Spring 2006

16

Hacker Methodology

- Identifying a Victim
- Casing the Joint
- Gaining Access
- Executing the Attack

GMU ISA 774 Spring 2006

17

Security Engineering vs Traditional Engineering

- Traditional Engineering
 - Designing products and processes that do useful things
- Security Engineering
 - Designing systems to operate effectively and maintaining “CIA” despite poor requirements, uncertainty, hostile environments, and bad Karma

GMU ISA 774 Spring 2006

18

Rules for Intrusion Detection Systems

- IDS's operate in a hostile environment
- The IDS must be placed on a trusted platform
- Information sources must be reliable
- Some operations may be subject to legal challenge
- The IDS can't be too hard to use, or it won't be used
- The IDS itself should be audited
- The IDS must be operated in a manner consistent with law
- The IDS will eventually fail

GMU ISA 774 Spring 2006

19

9. Legal Issues

GMU ISA 774 Spring 2006

20

Legislation

- Laws covering computer crime must change and adapt constantly
- State and local statutes must also be considered, but
 - Poorly resourced
 - Poorly trained
- Victims hesitate to report computer crime
 - Why?

GMU ISA 774 Spring 2006

21

Legislation

- Computer Fraud and Abuse Act of 1984
- Electronics Communications Privacy Act
- National Infrastructure Protection Act of 1996
- Clinger Cohen Act
- HIPAA
- Sarbanes Oxley
- FISMA

GMU ISA 774 Spring 2006

22

Computer Fraud and Abuse Act of 1984

- Amended in 1996 by the National Infrastructure Protection Act
- Criminalizes certain activities that effect computer systems
 - Unauthorized access
 - Information theft
 - Unauthorized modification of systems or their contents

GMU ISA 774 Spring 2006

23

Electronics Communications Privacy Act of 1986

- Amends Privacy Act on access, use, disclosure, interception, and privacy protection of electronic, wire, or oral communications.
- Designed to expand protection to apply to new technologies *radio paging devices, electronic mail, cellular telephones, private communication carriers, and computer transmissions.*
- Excludes service providers so they may use wire or electronic communications in activities necessary to support the service or to protect their rights or property but cannot observe or randomly monitor except for mechanical or service quality control checks.
- Outlines what needs to be provided by law enforcement to compel the service provider to provide information....

GMU ISA 774 Spring 2006

24

The Clinger-Cohen Act of 1996

- Establish an Electronic Government
- Major changes to IT acquisition:
- Requires the government IT shop to operate exactly as an efficient and profitable business would
- Acquisition, planning and management of technology must be treated as a "capital investment."

GMU ISA 774 Spring 2006

25

The Clinger-Cohen Act of 1996

- The CIO must
 - Have technical, financial and communications skills
 - Determine that proposed investment supports Agency's mission.
 - Show that the Agency can perform the function, rather than outsource
 - Ensure business processes have been redesigned for efficiency

GMU ISA 774 Spring 2006

26

Civil Litigation/Tort Law

- Allows victims to be compensated when injured
- Administrative and civil actions have been prevalent in cases of economic crime
- Possible Concerns
 - Litigation for unsuccessful security
 - Downstream liability
 - Liability from erroneous intrusion detection response action

GMU ISA 774 Spring 2006

27

Rules of Evidence

- Types of Evidence
- Admissibility of Evidence
- Restrictions and Exceptions
- Provisions for Handling Evidence
- Rules of Evidence as Applied to System Logs And Audit Trails

GMU ISA 774 Spring 2006

28

Rules of Evidence

- Restrictions and Exceptions
 - Business records
 - Personal knowledge not required
 - Photographic copies
- Provisions for Handling Evidence
 - Must follow the chain of custody
- Rules of Evidence as Applied to System Logs And Audit Trails
 - Best practice is the have a comprehensive monitoring policy and procedures that follow that policy

GMU ISA 774 Spring 2006

29

Laws Relating to Monitoring Activity

- System Administrators
 - Sysadmin monitoring (random) is allowed by the ECPA
 - Other requirements exist
- Law Enforcement
 - In general, need a warrant
- Notification of Monitoring
 - Include in consent to use documents
 - Should be a publicized part of the security policy

GMU ISA 774 Spring 2006

30

Real Cases

- Lessons Learned
 - The goals of ID may be at odds with legal restrictions
 - Involve your legal department with issues of monitoring policies and techniques
 - Intrusion detection administrators should receive regular briefings on applicable law
 - Have response policies in place before you need them

GMU ISA 774 Spring 2006

31

Evaluating IDS

GMU ISA 774 Spring 2006

32

Measurement Criteria

- Ability to identify attacks
- Stability, Reliability and Security
- Information provided to analyst
- Manageability
- Scalability and interoperability
- Vendor support

GMU ISA 774 Spring 2006

33

IDS Testing Methodology

- Purpose of testing
 - Developers
 - Researchers
 - Customers
- Requirements and Metrics
 - Requirement: Does feature X work?
 - Metric: Does feature X meet this measure?

GMU ISA 774 Spring 2006

34

IDS Testing Data

- Simulated attack data
- Sample of real world traffic
- Can we really measure IDS coverage?
- Attack Traffic Generation
 - Provides a reusable set of traffic and attacks useful for IDS performance comparison
 - Can this ever really simulate real traffic?
 - Well known data sets had artifacts that made attacks easy to spot

GMU ISA 774 Spring 2006

35

IDS Testing

- Evaluating any new system before deployment is necessary
- Evaluating IDS presents particular challenges
- The desired benefits of the evaluation must be offset by the resources required

GMU ISA 774 Spring 2006

36

10. Considerations For Users

GMU ISA 774 Spring 2006

37

Determining Your Requirements

- Your System Environment
- Goals and Objectives
- Reviewing Your Policy
- Requirements and Constraints
 - External Requirements
 - Resource Constraints

GMU ISA 774 Spring 2006

38

Making Sense of Products

- The Problem Space
- Is the Product Scalable?
- How Did you Test this?
- Tool or Application?
- Buzzwords vs. Wisdom
- Anticipated Life of Product
- Training Support
- Goals of the Product
- Product Differentiation

GMU ISA 774 Spring 2006

39

Mapping Policy to Configurations

- Converting Policy to Rules
- Subject-Objects to Real World
- Monitoring Policy vs Security Policy
- Testing Assertions

GMU ISA 774 Spring 2006

40

Incident Handling and Investigation

- Preparation!!!
- Best Practices
- When the Balloon Goes Up
- Dealing with Law Enforcement
- Expectations
- Damage Control
- Dealing with Witch Hunts

GMU ISA 774 Spring 2006

41

11. Considerations For Strategists

GMU ISA 774 Spring 2006

42

Building Case for Security

- Assemble information
- Organizational Goals
- Security's fit into the Business Goals
- Security's fit with Risk Management
- Determining security needs
- Corporate Champions
 - Internal audit, legal, security, marketing
- Overcoming REsistance

GMU ISA 774 Spring 2006

43

Defining Requirements for IDS

- Revisiting Goals and Objectives
- What are the Threats?
- What are our Limitations?
- Considerations in Adopting ID and System Monitoring
 - User Privacy
 - Private data (HIIPA, Privacy Act)
- Marketing Hype vs. Real Solutions

GMU ISA 774 Spring 2006

44

The Effects Of Corporate Transitions

- Mergers and Acquisitions
 - Department of Homeland Security
- Strategic Partners
- Globalization
- Expansion and Contraction
- Going from Private to Public

GMU ISA 774 Spring 2006

45

12. Considerations For Designers

GMU ISA 774 Spring 2006

46

Requirements

- Good vs. Great ID
 - Effective
 - Easy to Use
 - Adaptable
 - Robust
 - Fast
 - Efficient
 - Safe

GMU ISA 774 Spring 2006

47

Requirements (con't)

- Different Approaches to Security
 - Control Function
 - Risk Management
 - Ecology
 - Think of the interactions of the entire environment
 - Transfer Function
- Policies – One Size Does Not Fit All

GMU ISA 774 Spring 2006

48

Security Design Principles

- Economy of Mechanism
- Fail Safe Defaults
- Complete Mediation
- Open Design
- Separation of Privilege
- Least Privilege
- Least Common Mechanism
- Psychological Acceptability

GMU ISA 774 Spring 2006

49

Best Practices

- Use Good Engineering Practices
- Secure Sensors
- Pay Attention to Correct Reassembly
- Don't Underestimate Hardware Needs
- Don't Expect Trusted Sources of Attack Data
- Think Through Countermeasures
- No Support for Forensics
- Support Modern Security Features

GMU ISA 774 Spring 2006

50

IDS for Wireless Networks

- Threats
 - Rouge Wireless Access Points (WAPs)
 - Denial of Service Attacks
 - Weak Encryption

GMU ISA 774 Spring 2006

51

Wireless IDS Issues

- Architecture
 - Distributed
 - Centralized
- Physical Response Needs
 - Attackers are somewhere close!!!
 - Use IDS technology to provide location data
 - Response team with mobile IDS technology

GMU ISA 774 Spring 2006

52

Wireless IDS Issues

- **Wireless IDS Benefits**
 - Identify rogue access points
 - Provide data to physically locate attackers
 - Identify other wireless threats
- **Wireless IDS Drawbacks**
 - A new, complex technology
 - Potential cost
 - Staff training and experience requirements

GMU ISA 774 Spring 2006

53

Wireless Network Issues

- **Lack of Physical Wires**
- **Limited Bandwidth**
- **Difficulty in differentiating anomaly and normal operation**
- **Communication security between nodes**

GMU ISA 774 Spring 2006

54

IDS Issues for Ad Hoc Networks

- **No Centralized Access or Audit Point**
 - No consolidated database of attack data
 - Coordination overhead between nodes
 - Must use distributed ID algorithms
- **Greater Potential of Node Compromise**
 - High value nodes
 - Compromising one node may corrupt or delay the trust relationships
 - May result in temporary DOS
- **Difficulty Obtaining Sufficient Audit Data to Perform ID**
 - Less communication between mobile nodes compared to fixed nodes
 - Difficult to establish a pattern of normal activity

GMU ISA 774 Spring 2006

55

13. Future Needs

GMU ISA 774 Spring 2006

56

Future Trends in Society

- Global Villages and Marketplaces
- Privacy as an Economic Driver
- A Different Kind of War
- Sovereignty

GMU ISA 774 Spring 2006

57

Future Trends in Technology

- Changes in the Network Fabric
- Open Source Software
- Advances in Wireless Networking
- Ubiquitous Computing

GMU ISA 774 Spring 2006

58

Future Trends in Security

- Management
- Privacy-Sparing Security
- Information Quality vs. Access Control
- Crypto, Crypto Everywhere
- The Erosion of Perimeters
- Liability Transfer vs. Trust Management

GMU ISA 774 Spring 2006

59

A Vision for Intrusion Detection

- Capabilities
- Highly distributed Architectures
- 911 for Security Management
- Ubiquitous Information Sources
- Silicon Guards
- Emphasis on Service, Not Product

GMU ISA 774 Spring 2006

60