

---

# Intrusion Detection

ISA 774  
George Mason University  
Spring 2006

---

## Week 13 Agenda

- Homework #2 Review
- Bace, Chapter 10, 11, 12
  - Considerations for Users, Strategists and Designers
- Assigned Reading
  - *An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks*, Andrew B. Smith, Mississippi State University
  - *Insertion, Evasion and Denial Of Service:-Eluding Network Intrusion Detection System*, Thomas H. Ptacek, Timothy N. Newsham.

Please put cell phones, pagers, etc on silent

GMU ISA 774 Spring 2006 2

---

## Homework #2

- Briefly describe honeypots and honeynets.
  - What are some of the benefits of these systems?
  - What are some of the drawbacks?
- What are some of the problems in evaluating intrusion detection systems?
- What are 2 legal issues that may effect how you operate or administer your intrusion detection environment?

GMU ISA 774 Spring 2006 3

---

## Homework #2

- Install a CD-ROM/DVD “live distribution” of a Linux or UNIX based security operating system on your PC. Use the available tools to assess the security of your system. Answer the following questions:
  - Which distribution did you choose? Why?
  - What tools are available on the distribution that can be useful in intrusion detection?
  - What benefits are there to using these canned distributions for intrusion detection?
  - What drawbacks are there to using these distributions?

GMU ISA 774 Spring 2006 4

## Security Live CDs

GMU ISA 774 Spring 2006 5

## Federal Plan for Cyber Security and Information Assurance Research and Development

---

The Cyber Security and Information Assurance Interagency Working Group of the National Science and Technology Council recently released a draft of their [Federal Plan for Cyber Security and Information Assurance Research and Development](#).

The approach calls for increased interagency R&D efforts and collaboration with the private sector to create a technical framework for a coordinated approach to R&D in cyber security and information assurance with the purpose of strengthening the Nation's IT Infrastructure.

Public comments on the Plan may be sent to [csia-plan-comments@nitr.gov](mailto:csia-plan-comments@nitr.gov) before April 28, 2006.

GMU ISA 774 Spring 2006 6

## 10. Considerations For Users

---

GMU ISA 774 Spring 2006 7

## Determining Your Requirements

---

- Your System Environment
  - System Configurations
  - Security Configurations
- Goals and Objectives
  - Protect from Outsiders
  - Protect from Insiders
  - Determine new technology or security needs
  - Maintain managerial control
    - Internet Filtering Filtering

GMU ISA 774 Spring 2006 8

## Determining Your Requirements

---

- Reviewing Your Policy
  - Goals
  - Job Descriptions
  - Use Standards
  - Formality or Organizational Maturity
- Requirements and Constraints
  - External Requirements
    - Standards and laws
    - Accreditation
  - Resource Constraints

GMU ISA 774 Spring 2006

9

## 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

10

## 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

11

## 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

12

## 11. Considerations For Strategists

---

GMU ISA 774 Spring 2006

13

## 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

14

## 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)

GMU ISA 774 Spring 2006

15

## Marketing Hype vs. Real Solutions

---

- What Product is the Best Fit for Us?
- How Painful is the Installation?
- How Painful is it to Run?
- What is Expected from Personnel?
- Who was this System Designed For?

GMU ISA 774 Spring 2006

16

## 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 17

## 12. Considerations For Designers

---

GMU ISA 774 Spring 2006 18

## Requirements

---

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

GMU ISA 774 Spring 2006 19

## 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 20

## 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

21

## Surviving the Design Process

---

- Establishing Priorities
  - Constrain what you think you can actually accomplish
- On Threat Curmudgeons
  - Fully understand the potential of attackers
- Striking and Maintaining Balance

GMU ISA 774 Spring 2006

22

## Metrics (Painting the Bulls Eye)

---

- Gauging Success
- False Starts
- Testing Approaches
- Measuring Network-Based Performance

GMU ISA 774 Spring 2006

23

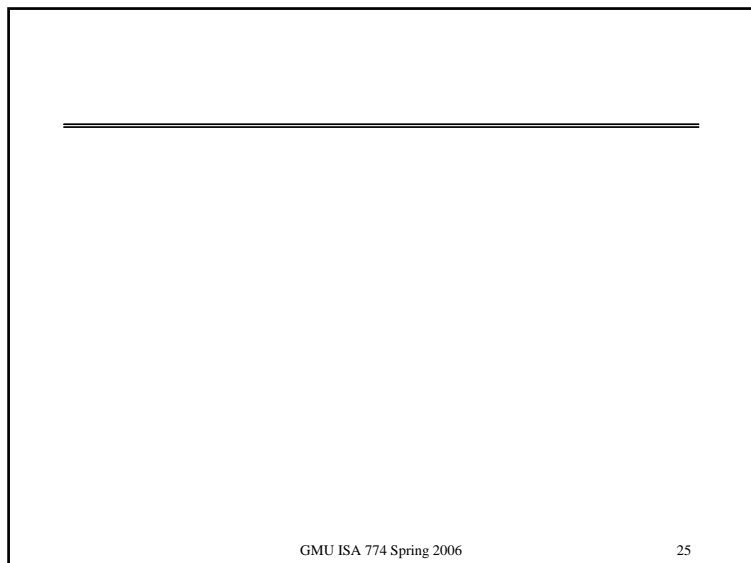
## Advice from the Trenches

---

- 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

24



## IDS for Wireless Networks

---

- Threats
  - Rouge Wireless Access Points (WAPs)
    - Attacker
      - WLAN Spoofing
    - Local User
      - Create a network back door
  - Denial of Service Attacks
  - Weak Encryption
    - WEP key susceptible to brute force attack

GMU ISA 774 Spring 2006 26

## 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 27

## 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 28

## Wireless IDS Products

---

- Commercial
  - AirDefense Guard
  - ISS Wireless Scanner
- Open Source
  - Snort-Wireless
  - WIDZ
- “Homegrown” Systems

GMU ISA 774 Spring 2006

29

## Snort-Wireless Preprocessors

---


- **Null SSID - AntiStumbler** - Programs such as NetStumbler and MacStumbler utilize **null SSIDs** in order to discover other access points. These are SSIDs coax other access points into returning their SSIDs to the broadcasting host. This is useful for wardriving and other network reconnaissance attempts.
- **DeauthFlood** - The attack detailed in Humphrey Cheung's article on [how to crack WEP](#) uses a **deauthentication flood** to get hosts to disassociate with a given access point and attempt to reauthenticate, thereby generating more packets to help with a WEP [cracking](#) attempt. This can also be used as a **Denial of Service (DoS)** attack against the access point.
- **AuthFlood** - Similar to DeauthFlood, the AuthFlood preprocessor detects and alerts against authentication flooding attacks, which involve a client attempting to associate with the wireless network many times and can be used to DoS the access point.
- **MacSpoof** - One of the most effective ways to limit access to an access point is to set up 'white lists' of MAC addresses that can associate with the access point, and include all others. The MacSpoof preprocessor examines the sequence numbers of packets received for any anomalies that hint at spoofed MAC addresses and generates an alert.
- **RogueAP** - Rogue access points are malicious access points that attempt to masquerade as benign access points in order to get a user to authenticate with them and unknowingly give up sensitive personal information.

GMU ISA 774 Spring 2006

30

## Open Source Wireless IDS Hack

---

- Linksys WRT54G wireless router 
  - Runs open source firmware
- Install OpenWRT RC 2
  - A small light system similar to Debian Linux
- Install Snort-Wireless
  - Similar to Snort
  - Deployed on a WAP to detect wireless attacks
- See excellent article “How To: Sniffing the Air”

GMU ISA 774 Spring 2006

31

## IDS in Mobile Ad Hoc Networks

---

*Discussion of An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks,*  
Andrew B. Smith, Mississippi State University

- Ad Hoc Networks
  - Mobile nodes that communicate in an indeterminate pattern
  - No fixed controlling node
- Ad Hoc Mobile Network Examples
  - Military strike components
  - Emergency service responders
  - Trucking and delivery services

GMU ISA 774 Spring 2006

32

## Wireless Network Issues

- Lack of Physical Wires
  - Eavesdropping a definite possibility
  - Jamming a key node can block collaborative IDS
- Limited Bandwidth
  - IDS function can only use a small portion of wireless network bandwidth
  - Transmission delays to distant nodes
- Difficulty in differentiating anomaly and normal operation
  - Rogue node or just a late update?
- Communication security between nodes
  - Must use strong encryption
  - Need most efficient algorithms
    - Public key too resource intensive

GMU ISA 774 Spring 2006

33

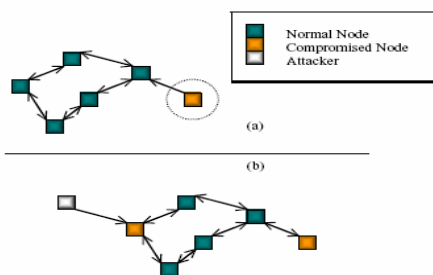
## IDS Issues for Ad Hoc Networks

- 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

34

## Ad Hoc Network Node Compromise



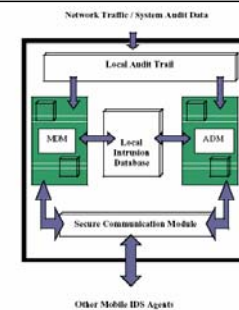
**Figure 1:** (a) An attacker has compromised a node of the network and forces other nodes to do a re-key. (b) While the network is slowed, another attacker attacks a different node, causing it to be compromised.

GMU ISA 774 Spring 2006

35

## Mobile IDS Network Architecture

- Mobile IDS Agents
  - Local Audit Trail
  - Local Intrusion Database
  - Secure Communication Module
  - Anomaly Detection Modules
  - Misuse Detection Modules
- Stationary Secure Database



**Figure 2:** A Graphical Representation of a Proposed Mobile IDS Agent

GMU ISA 774 Spring 2006

36

## Mobile IDS Network Architecture

---

- Stationary Secure Database
  - Congregates ID data from agents
  - Contains the consolidated attack database
  - Must be in a very secure location

- Stationary Secure Database Issues
  - Agents must physically connect
  - Reduces possible physical footprint
  - What happens if compromised or lost?

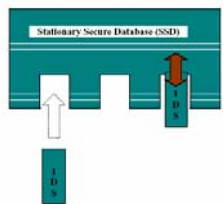


Figure 3: Mobile IDS Agents interacting with SSD

## Next Class

---

- Topics
  - Future of IDS
  - IDS Evasion
  - Honeynets and Honeypots
  - Other protocol environments
- Read
  - Bace, Chapter 13
  - *Towards a Third Generation Data Capture Architecture for Honeynets*, Edward Balas and Camilo Viecco, [The Honeynet Project]  
<http://www.honeynet.org/papers/individual/hflow.pdf>

## Additional Resources

---

- *Federal Plan for Cyber Security and Information Assurance Research and Development*. NIST.  
[http://www.nitrd.gov/pubs/csia/FederalPlan\\_CSIA\\_RnD.pdf](http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf)
- *How To: Sniffing the Air*, Derek Boiko-Weyrauch.  
[http://www.tomsnetworking.com/2005/09/28/how\\_to\\_snort/](http://www.tomsnetworking.com/2005/09/28/how_to_snort/)
- *10 Best Security Live CD Distros (Pen-Test, Forensics & Recovery)*.  
<http://www.darknet.org.uk.nyud.net:8090/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery/>
- *Know Your Enemy: Honeynets – What a honeynet is, its value, and risk/issues involved*. Honeynet Project.  
<http://www.honeynet.org/papers/honeynet/>