THE INSTITUTE
FOR APPLIED NETWORK SECURITY

Information Assurance Track ②

IATAC
Information Assurance
Technology Analysis Center

Deterring the Insider Threat – Honest mistakes vs. malicious insiders

March 5-6, 2007
Mid-Atlantic Information Security Forum
Tysons Corner, VA

Dr. Bruce Gabrielson
Dr. Ron Ritchey

Curriculum Map - Monday

Information Protection	Identity & Access Management	Enterprise Defense	Information Assurance (IATAC)	Regulatory Environment	MBA in a Day
Data Leak Technology: Can it live up to the hype?	Authentication: Drivers for adoption (FFIEC) & review of leading technologies	Network Architecture best practices: segmentation techniques, organizational issues	Software Assurance – Are quality, dependability and security achievable?	Compliance spending: Too much, too little, just right? How do you know?	Baking Security into Your Organization
Messaging Security	Authorization & Provisioning	Advanced SIM Management	Deterring the Insider Threat – Honest mistakes vs. malicious insiders	E-discovery: Are you ready for the new rules?	Speaking "Security" to Executives – Getting Creative
Database Security	Convergence of Physical and Digital Access Management	Configuration & Patch Management	NetOps – Bringing disparate operational capabilities into a cohesive entity	Current events: what will TJX mean for 2007?	Security Productivity & Metrics

Discussion Objectives

- Overview of the Problem Space
- Open discussion on how the threat is perceived (Government, Academic and Commercial)
- Open discussion on activities that should be detected or monitored and where
- Open discussion on how false positives could be reduced

What is an Insider

As a general definition, the “insider” is anyone who is or has been authorized access to an information system.

- Persons who constitute insider threats range from incompetent users making critical mistakes to moles who have been recruited, trained, and planted by nefarious outsiders.
- Some definitions address the broader scope of insiders to include outsiders that compromise systems and then act as insiders (pseudo-insiders).

Critical Questions

What causes the most damage, mistakes or actual malicious insider activity?

How do the various communities view the most significant threats?

How are insiders detected and who should be responsible for investigating?

The best solution is: host only, network only, or both? (Limitations)

Why do you think it has taken so long for solutions to develop?

How could you differentiate between bad behavior and a malicious insider?

Critical Questions

Suggestions for handling false positives?

How can exfiltration be discovered?

What are some behavior traits that might indicate a potential insider?

In your opinion, is a cyber-based solution possible?

At what point does an internal investigation turn into a legal issue?

What community: DoD, Government, Health Care, Banking, or Industry is doing the most to reduce insider threats?

THE INSTITUTE
FOR APPLIED NETWORK SECURITY