A Tamper-resistant Monitoring Framework for Anomaly Detection in Computer Systems

S. Upadhyaya

Computer Science & Eng.
University at Buffalo
Buffalo, New York, 14260

Outline

- General Background
- A New Intrusion Detection Strategy
- Tamper-resistant Monitoring
- Some Experimental Results
- Center of Excellence in IA at Buffalo
- Research and Educational Activities

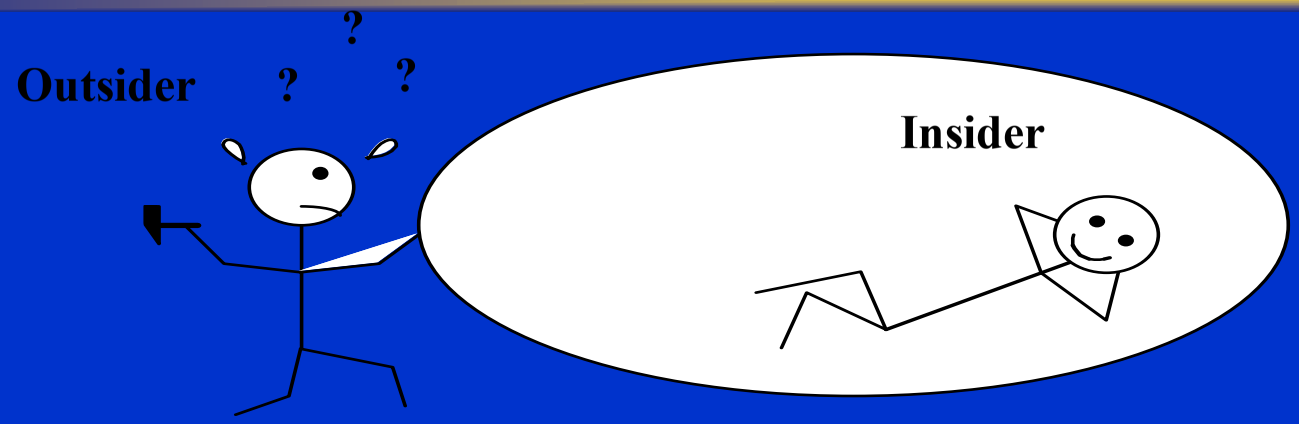
Basic Terminologies

- A *Host*
  - A computer system
- A *Service*
  - A user space program that performs some useful task
- A *Vulnerability*
  - A flaw in a program with security implications
  - An Attacker targets vulnerabilities in programs to gain elevated privileges
- An *intrusion detection system* (IDS) attempts to detect and prevent attacks

Cyberspace Threats and Vulnerabilities

- Hacking in 2000 brought down Yahoo, Amazon, CNN.com etc.
  - Cost millions of $ in lost revenues
- NIMDA virus a week after the Sept. 11 attack
  - Struck leading financial services firms
  - Went nationwide, lasted for 5 days, attacked 86,000 computers
  - Forced firms offline, denied customer access
- Sources estimate the impact of cyber attacks in $13 billion in 2001
- Insider Threats

External Vs. Internal



- **Outsider**
  - Needs access to system
  - Works quickly to avoid detection
  - Installs trapdoors for further access
  - Works in unfamiliar environment
- **Insider**
  - Has access to system
  - Works leisurely
  - Future access guaranteed
  - Works in familiar environment
  - Knows what is important

Measures Taken by the U.S. Government

- Targeting Cyberterrorism
  - October 1997, President's Commission on CIP
  - Identifies nation's electrical, transportation, telecom & financial systems as critical points
  - Need to be made secure and dependable
- Information Security Summit at White House, Feb. 2000
  - Goal was to find ways to defeat distributed DOS
- Cyber security a national level effort, 2002
- National strategy was unveiled in Sept. 2002

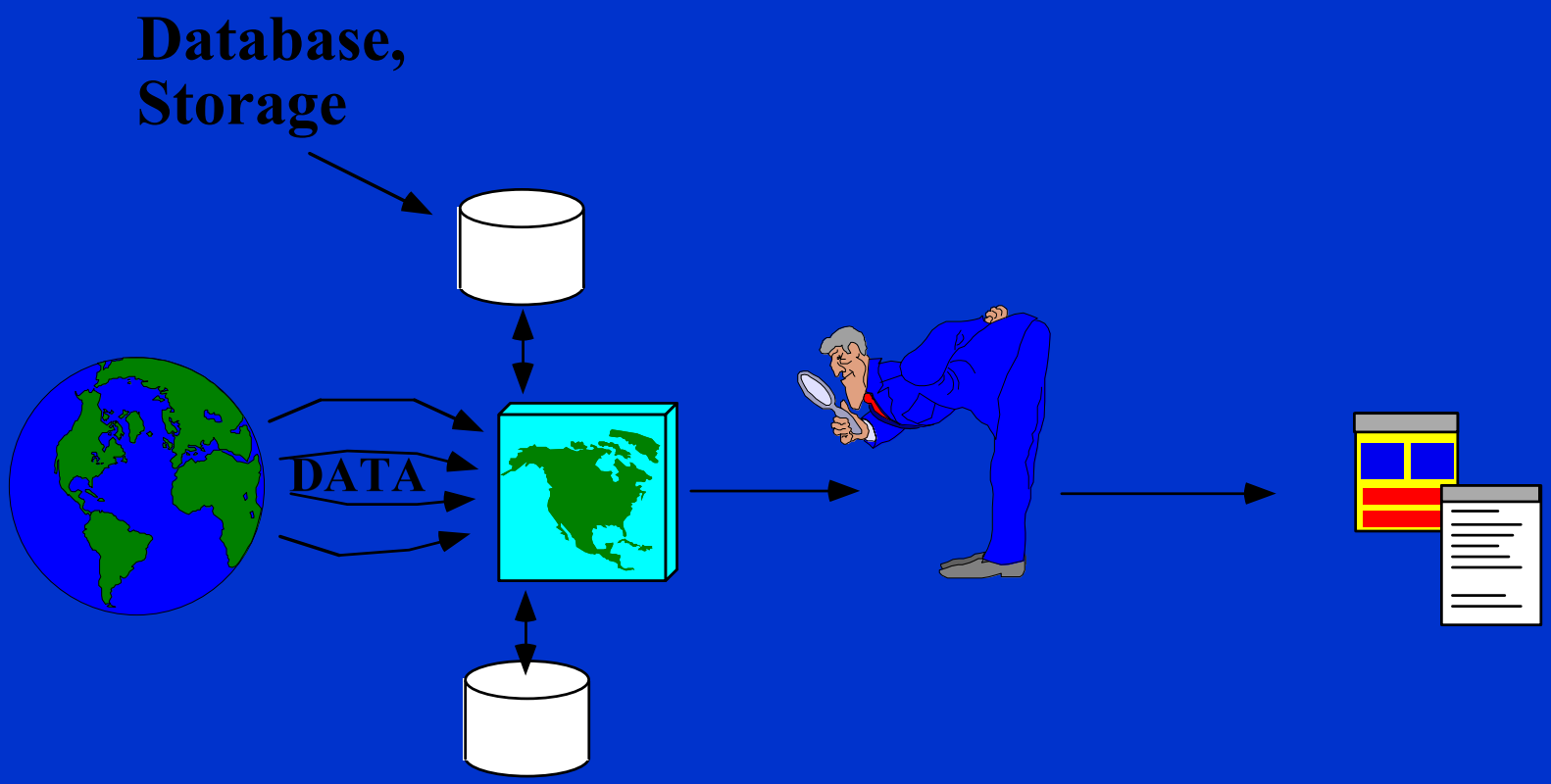
Cryptographic Techniques

- Computer crime is certain to continue
- Institute controls to preserve
  - Confidentiality, Integrity, Availability
- Encryption is the most powerful tool
- Strongly based on Information Theory
- Heavily researched topic - RSA Scheme, Elliptic Curve
- It doesn't solve all the security problems
- Need to develop counter-measures that would complement existing schemes

What is IDS?

- In its general sense --
  - Acquires information about its environment to analyze system behavior
  - Aims to discover security breaches, attempted breaches, open vulnerabilities that could lead to potential breaches
- Types of information –
  - Long term info. – a knowledge base of attacks (static)
  - Configuration info. – a model of the current state (static)
  - Audit info. – describing the events happening (dynamic)

IDS Architecture

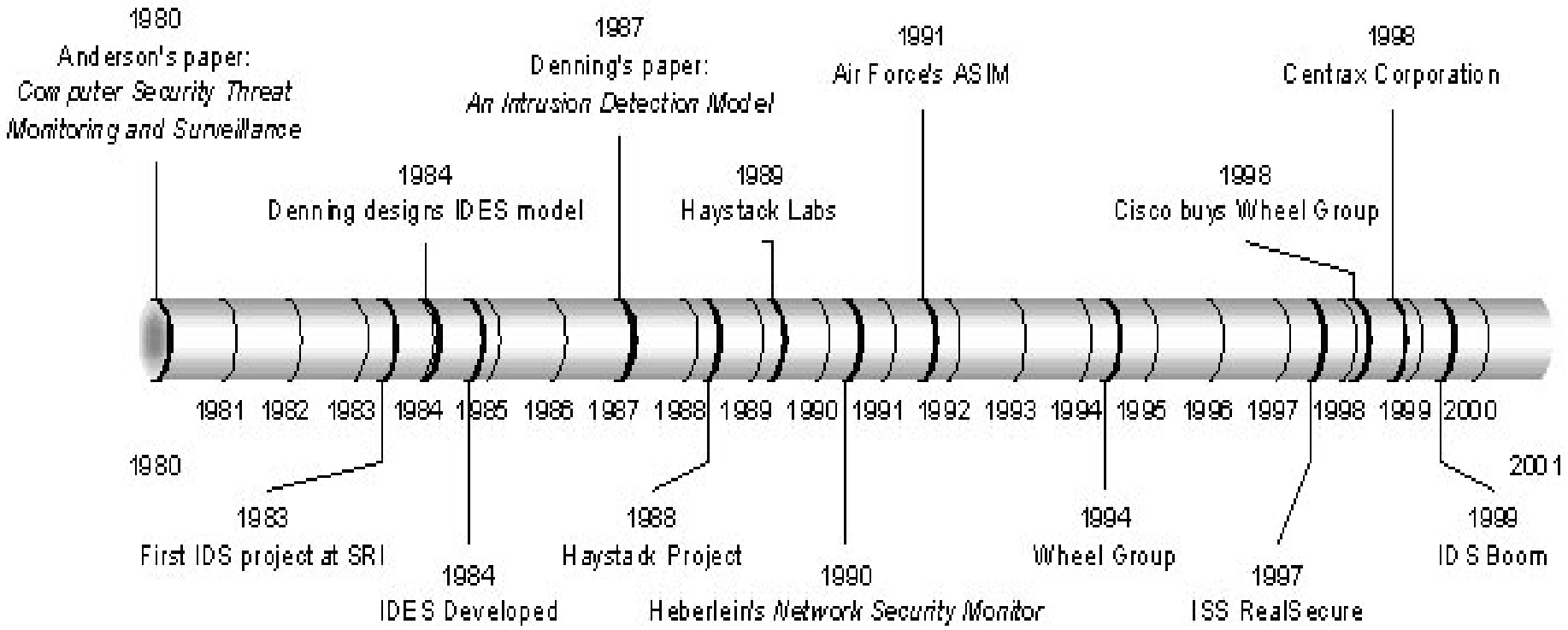


Approaches to Intrusion Detection

- Intrusion Detection –
  - Pioneered by D. Denning at SRI International
  - Misuse detection and anomaly detection
- Misuse Detection –
  - Called knowledge-based detectors
  - Uses a defined set of rules crafted to catch a specific malicious event
- Anomaly Detection –
  - Called behavior-based detectors
  - Raises an alarm for strange system behavior
  - Need a baseline for monitoring

Evolution of IDS

Paul Innella, CISSP's timeline:

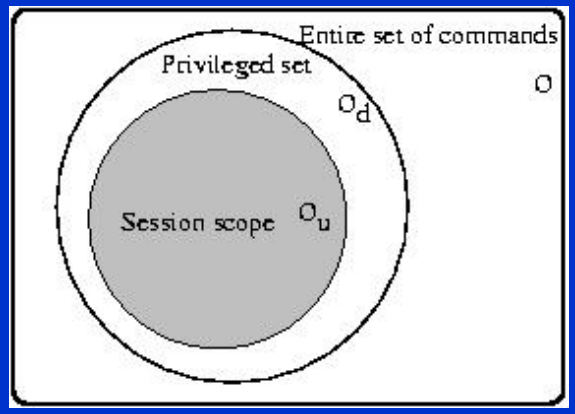


Limitations of Current Approaches

- Existing Intrusion detection techniques concentrate on sampling at low level
  - instrumentation is easy, but volumes of data
  - Huge computation
  - Semantics of user activities becomes diffuse
- Intrusion detection requires synthesis of this data
- Mostly after-the-fact

A New Approach

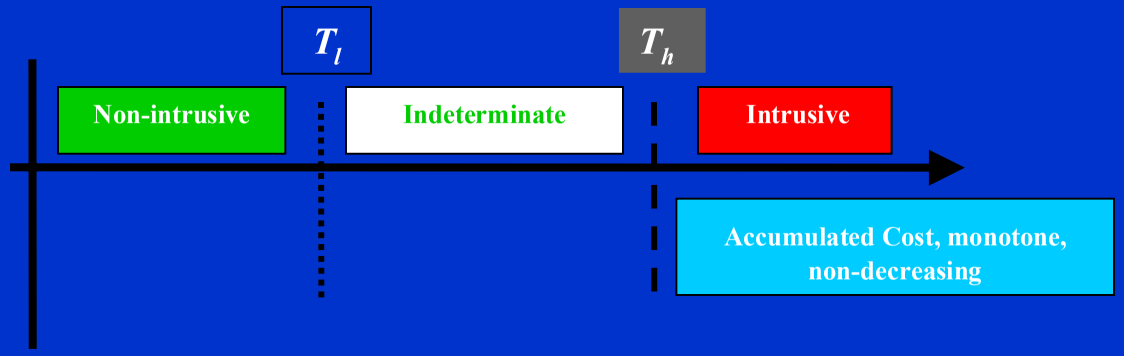
- Monitoring user activity at high level – user command level
- Supported by a query of user intent
  - Data to be monitored is small
- Starting with a session scope
  - With explicit query, we can define a smaller and personalized bracket of privileges or jobs for each user (Ou)



- Summary of work cited in national media by Associated Press (http://www.msnbc.com/news/861865.asp?0si=-&cp1=1)

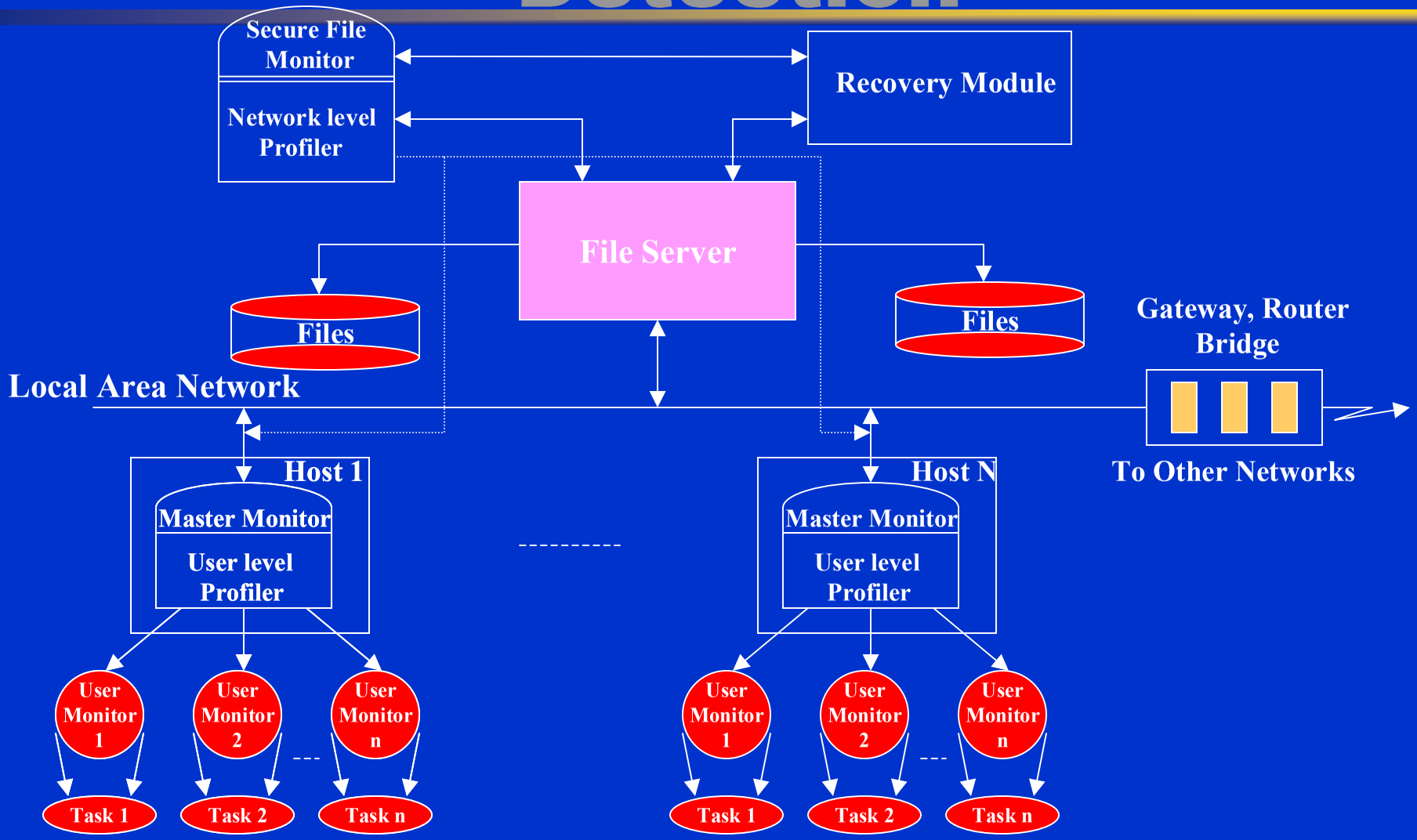
Reasoning About Intrusions

- Underlying principle
  - Legitimate user's computational habits rarely change abruptly leading to reasonably stable profile of activity for users
- Intrusion flagging is non-binary and reasoning about intrusions is essential to make informed decision
  - Cost analysis and reasoning



  - Window of uncertainty needs to be resolved quickly

Distributed Intrusion Detection

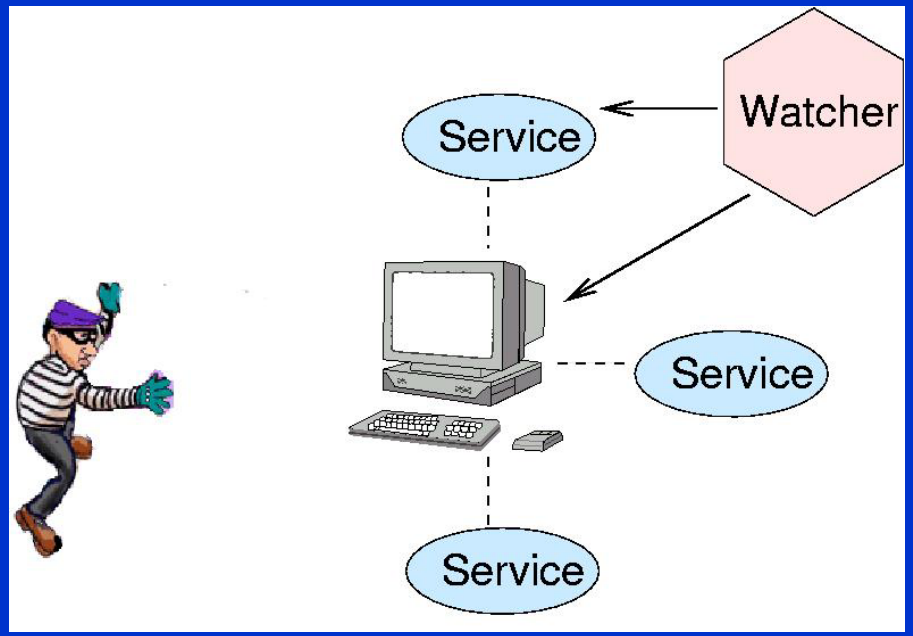


Summary of Experiments

Summary		1 User, No Multiple Logins	1 User, With Multiple Logins	2 Users, No Multiple Logins	2 Users, With Multiple Logins
User	Detection	87.50%	78.60%	74.90%	91.90%
and	Latency	33.4	35	36.1	29
User	False Positives	12.50%	21.40%	25.10%	8.10%
	False Negatives	0%	0%	0%	0%
User	Detection	98%	89%	100%	94.70%
and	Latency	0	11	0	9.6
Intruder	False Positives	0%	0%	0%	0%
	False Negatives	2%	11%	0%	5.30%
Intruder	Detection	99%	100%	98.20%	100%
and	Latency	0.4	0.7	0.6	0.5
User	False Positives	0%	0%	0%	0%
	False Negatives	1.40%	0%	1.80%	0%
Intruder	Detection	56%	81.30%	77.40%	91.50%
and	Latency	15.9	14.8	17	27
Intruder	False Positives	0%	0%	0%	0%
	False Negatives	44%	18.70%	22.60%	8.50%

Tamper-resistant Monitoring

- **Protecting user space components**
  - **To have secure enclaves, every component of IDS must be watched and there are no open ends**
  - **Who watches the watcher?**
- **Attacker's perspective**



The Attack Model

- An attacker is successful, if:
- He compromises the service running on the host
- He disables or compromises the IDS, if one is deployed
- Note:
  - Bypassing an IDS by taking advantage of its limited coverage is a known weakness and it is not a part of the attack model

Criteria for Analysis

- Failure due to faults and failure due to attacks are not one and the same
- Each software component can potentially fail due to attacks; we just don't know how yet!
- Security of a system is only as strong as the weakest link
- Hence, even if a service is monitored by a separate detection mechanism, is the entire setup really secure?
- An IDS is a program and it too can be compromised
- So, implement it inside the kernel for tamper-resistance
- Kernel implementations affect the whole system

Probabilistic Analysis

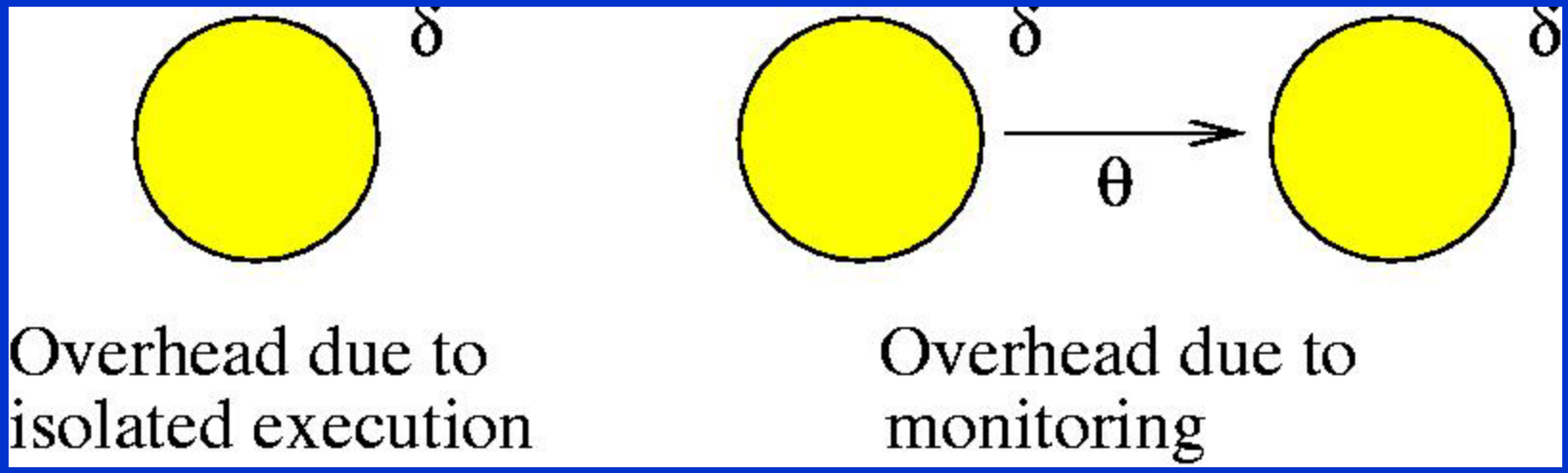
- An attacker has little knowledge about how the entire system works and the attacks are by trial and error
- Factors that determine the overall security are:
  - For each component, individual probability of failure
  - For a n component system, the total probability of failure
  - An attack can proceed in stages, per-stage probability of failure
  - Search space for a successful attack

Deterministic Analysis

- An attacker has complete knowledge of the system and its vulnerabilities
- Factors that determine the overall security are
  - A successful attack strategy

Performance Analysis

- If a detection mechanism is deployed, then how much overhead will it incur?

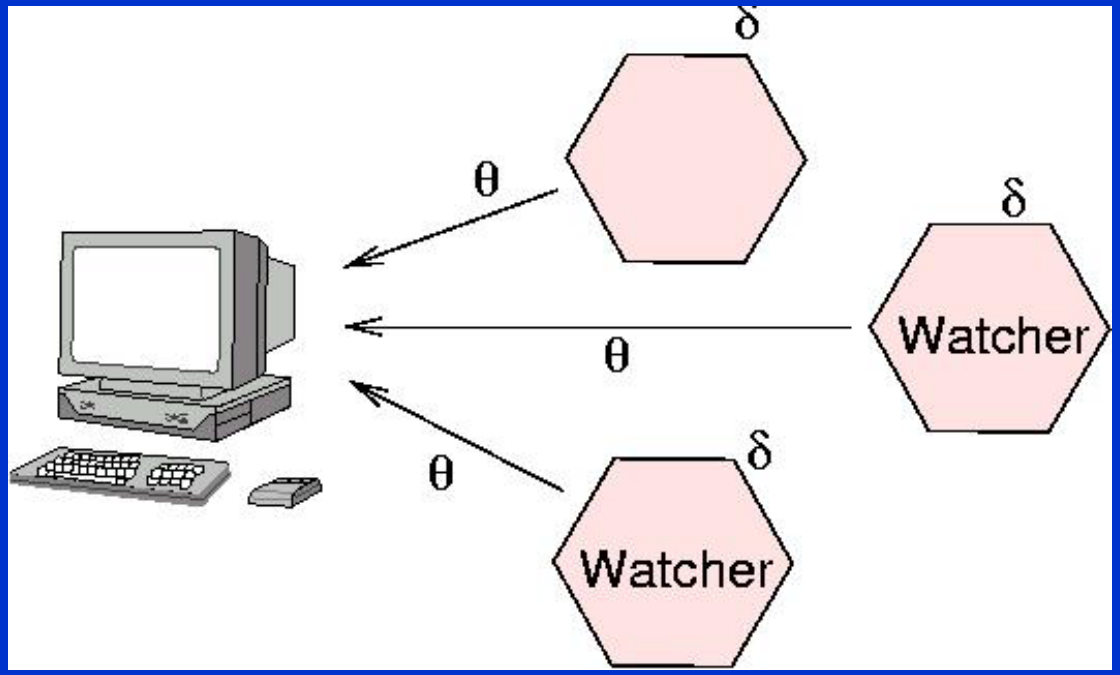


- delta- overhead due to isolated execution
- theta - overhead due to monitoring

Problem Transformation

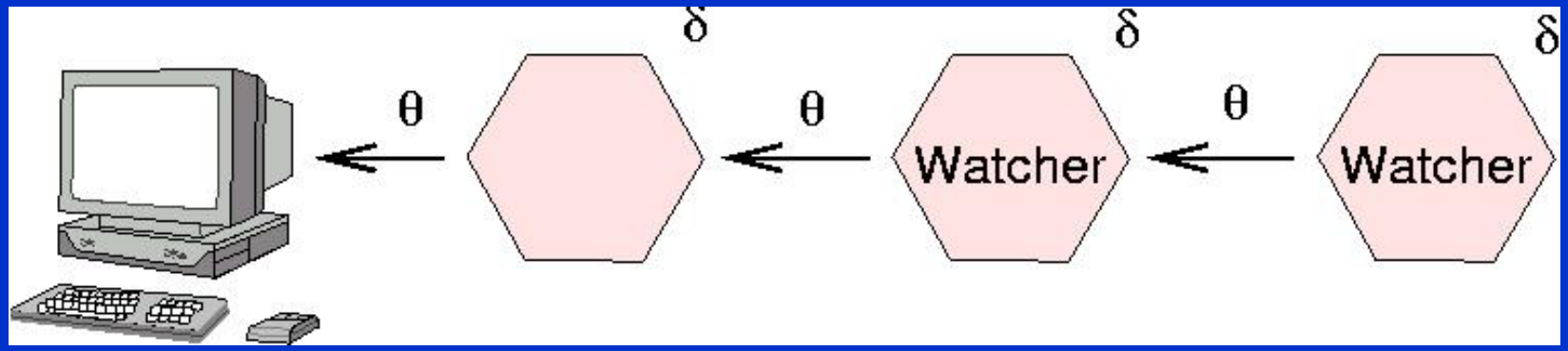
- Reduces to a graph problem
  - Each process is a node
  - Interaction between one process and another is a directed edge
- No mutual trust among processes

Simple Replication



- Chameleon project at UIUC
- Can be easily compromised

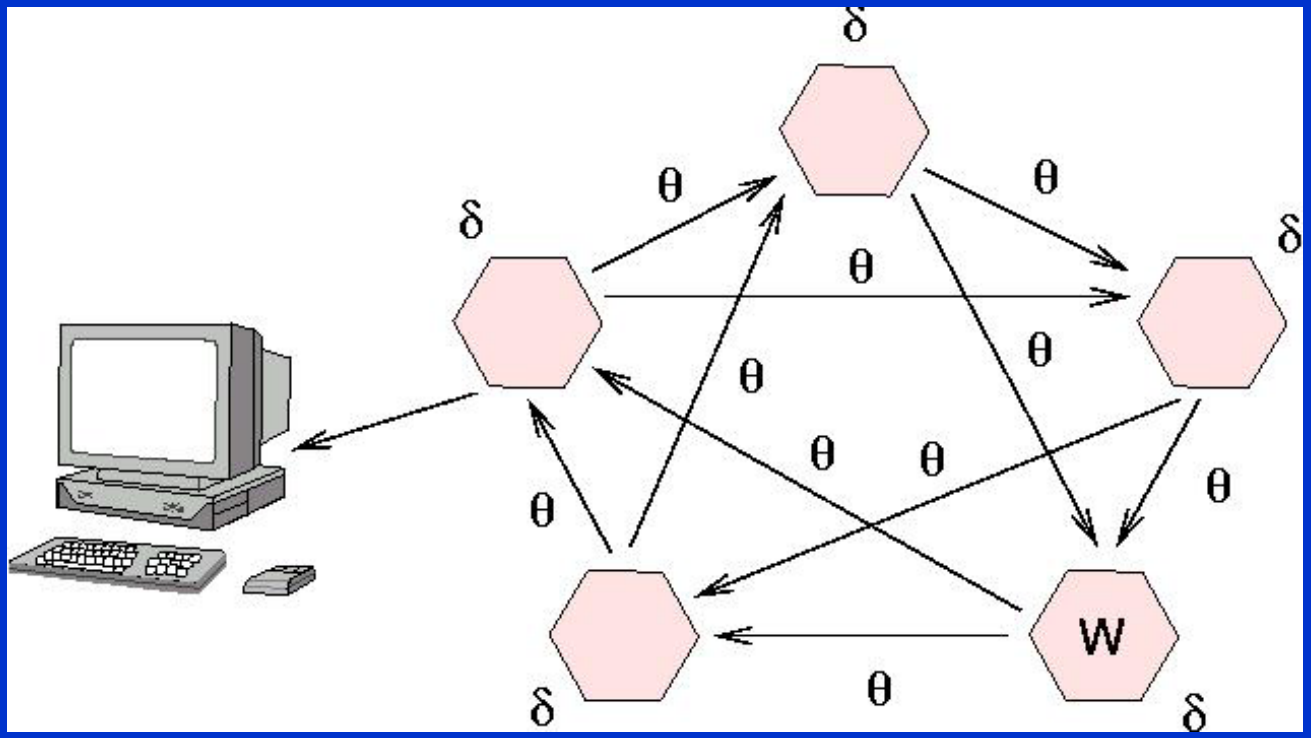
Layered Hierarchy



- An example is the AAFID project at Purdue
- Can be easily compromised

Circulant DiGraph

- New proposed architecture



- Very difficult to subvert
- Provides an infinite hierarchy of monitoring using finite no. of monitors

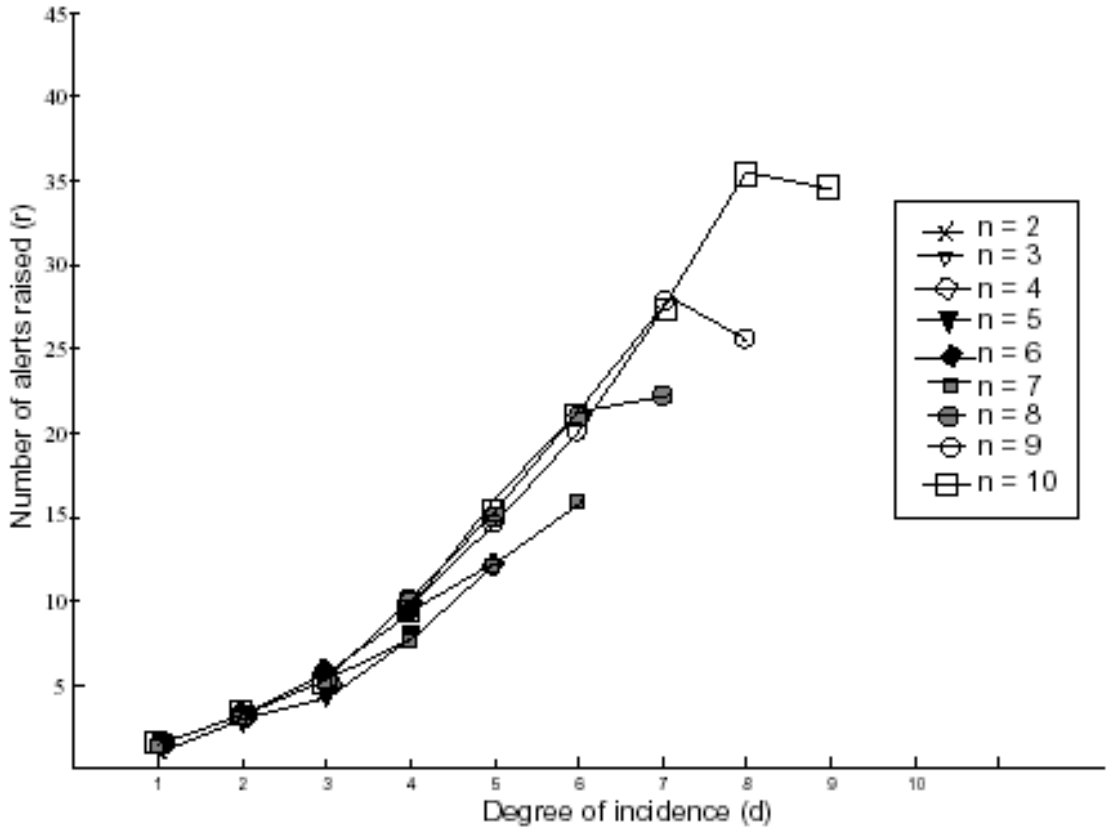
Comparison

Metrics	Simple Replication	Layered Hierarchy	Circulant Digraph
Subversion by sequential attack?	Yes	Yes	No
Total Probability of Subversion	p^n	p^n	p^n
Per-stage Probability of Subversion	p	p	p^n
Degree of Incidence	0	1	d
Overhead due to isolated execution	$n.\delta$	$n.\delta$	$n.\delta$
Overhead due to monitoring	$n.\theta$	$n.\theta$	$n.d.\theta$
Total overhead	$n.\delta + n.\theta$	$n.\delta + n.\theta$	$n.\delta + n.d.\theta$

Implementation

- Requires a sense-decide-act loop
- Uses FreeBSD's *kqueue* subsystem
- Each node in the graph is a process monitor
- Multiple outgoing edges from a node are threads

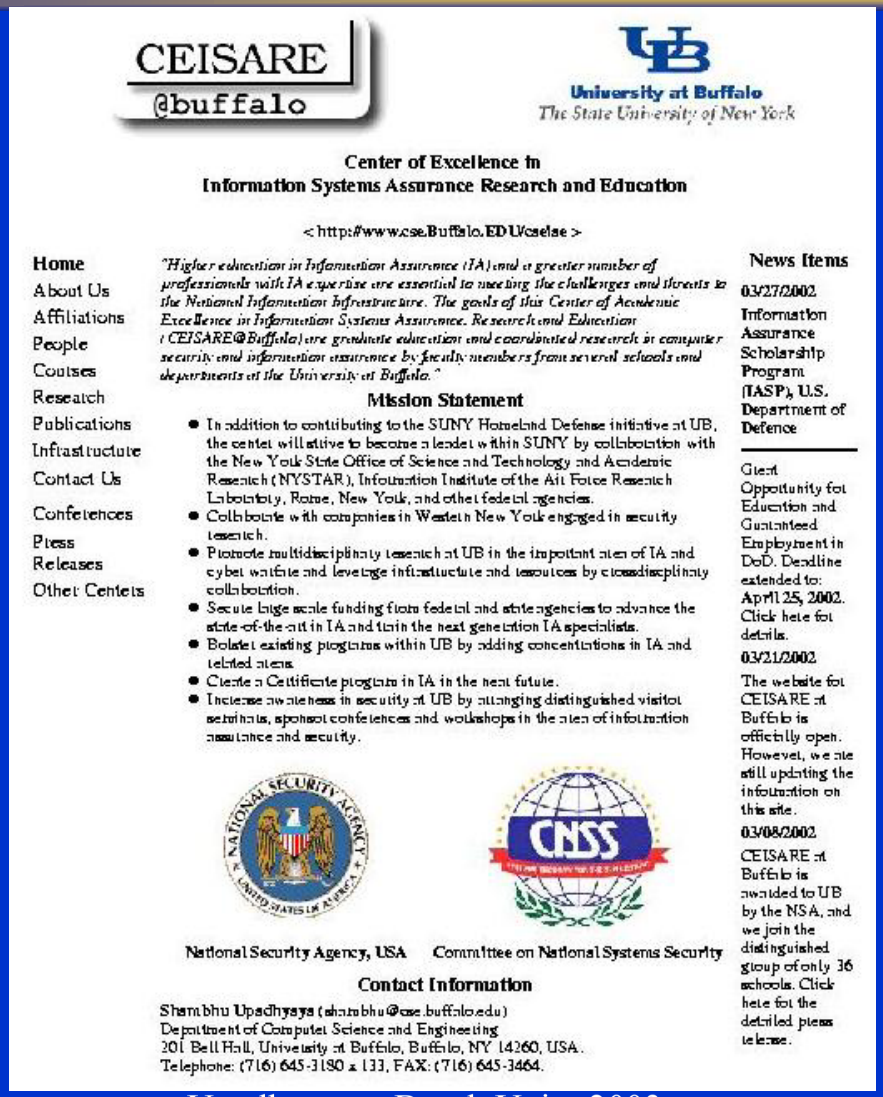
Results


Number of alerts raised (r)
Degree of incidence (d)
n = 2
n = 3
n = 4
n = 5
n = 6
n = 7
n = 8
n = 9
n = 10

Future Work

- The short term goal is to supplement the kqueue subsystem to support more events
- The long term goal is to devise a way to provide a generic tamper-resistant wrapper
- Extend it to network level monitoring
- Our website:
  - http://www.cse.buffalo.edu/caeiae/
- Other projects – security in mobile networks, biometrics authentication etc.

CEISARE Webpage



CEISARE @buffalo

University at Buffalo
The State University of New York

Center of Excellence in Information Systems Assurance Research and Education

< http://www.cse.Buffalo.EDU/cselse >

Home
About Us
Affiliations
People
Courses
Research
Publications
Infrastructure
Contact Us
Conferences
Press Releases
Other Centers

"Higher education in Information Assurance (IA) and a greater number of professionals with IA expertise are essential to meeting the challenges and threats to the National Information Infrastructure. The goals of this Center of Academic Excellence in Information Systems Assurance, Research and Education (CEISARE@Buffalo) are graduate education and coordinated research in computer security and information assurance by faculty members from several schools and departments at the University at Buffalo."

Mission Statement

- In addition to contributing to the SUNY Homeland Defense initiative at UB, the center will strive to become a leader within SUNY by collaboration with the New York State Office of Science and Technology and Academic Research (NYSTAR), Information Institute of the Air Force Research Laboratory, Rome, New York, and other federal agencies.
- Collaborate with companies in Western New York engaged in security research.
- Promote multidisciplinary research at UB in the important area of IA and cyber warfare and leverage infrastructure and resources by cross-disciplinary collaboration.
- Secure large scale funding from federal and state agencies to advance the state-of-the-art in IA and train the next generation IA specialists.
- Bolster existing programs within UB by adding concentrations in IA and related areas.
- Create a Certificate program in IA in the near future.
- Increase awareness in security at UB by arranging distinguished visitor seminars, sponsor conferences and workshops in the area of information assurance and security.

National Security Agency, USA Committee on National Systems Security

Contact Information

Shambhu Upadhyaya (shambhu@cse.buffalo.edu)
Department of Computer Science and Engineering
201 Bell Hall, University at Buffalo, Buffalo, NY 14260, USA.
Telephone: (716) 645-3180 x 133, FAX: (716) 645-3464.

News Items

03/27/2002
Information Assurance Scholarship Program (IASP), U.S. Department of Defence

Great Opportunity for Education and Guaranteed Employment in DoD. Deadline extended to: April 25, 2002. Click here for details.

03/21/2002
The website for CEISARE at Buffalo is officially open. However, we are still updating the information on this site.

03/08/2002
CEISARE at Buffalo is awarded to UB by the NSA, and we join the distinguished group of only 36 schools. Click here for the detailed press release.

Major Players -- Academia

- Purdue –
  - Eugene Spafford, Director of CERIAS
  - One of the four witness to testify before the House Science committee on infosec in 2001
  - Leads the center with about 5 faculty and numerous students and projects
  - Developed an IDS Using Autonomous Agents
- UC Davis –
  - Karl Levitt and Matt Bishop direct the security lab
  - Developed GrIDS (Graph based IDS)
- CMU – Home of CERT/CC
- Cornell
  - Language-based security led by F. Schneider

Major Players -- Industries

- IBM Watson, IBM Zurich --
  - Global Security Analysis Laboratory
  - Marc Dacier at Zurich leads the IDS projects
- Microsoft
  - Recently started the Trustworthy Computing initiative
- Cisco
  - Does research and development
  - Builds intrusion detection appliances – sensors and software

Major Players – Labs/Government

- SRI International --
  - Developer of EMERALD through funds from ITO, DARPA
- Air Force Research Lab --
  - Defensive Information Warfare Branch
- Naval Research Lab --
  - Center for High Assurance Computer Systems
  - Multi-level security
- National Institute of Standards and Technology --
  - Computer Security Resource Center
- National Security Agency --
  - Research and education

Popular Websites

- SANS (System Administration, Networking and Security) Institute
  - http://www.sans.org/aboutsans.php
- CERT/CC
  - http://www.cert.org/
- CERIAS (Center for Education and Research in Information Assurance and Security)
  - http://www.cerias.purdue.edu/
- NIST (National Institute of Standards and Tech.)
  - http://csrc.nist.gov/index.html