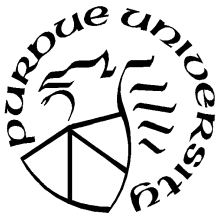
Purdue University

Center for Education and Research in Information Assurance and Security

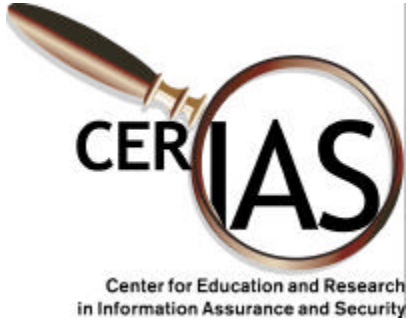


Denial of Service, Traceback and Anonymity

Clay Shields

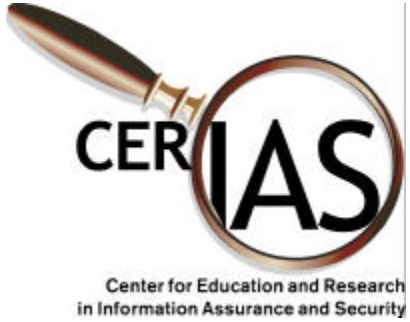
Assistant Professor of Computer Sciences

CERIAS



Network Security

- I am with CERIAS to look at network security issues
- Involved in a number of projects in the area
- Overview of research in context of denial-of-service attacks

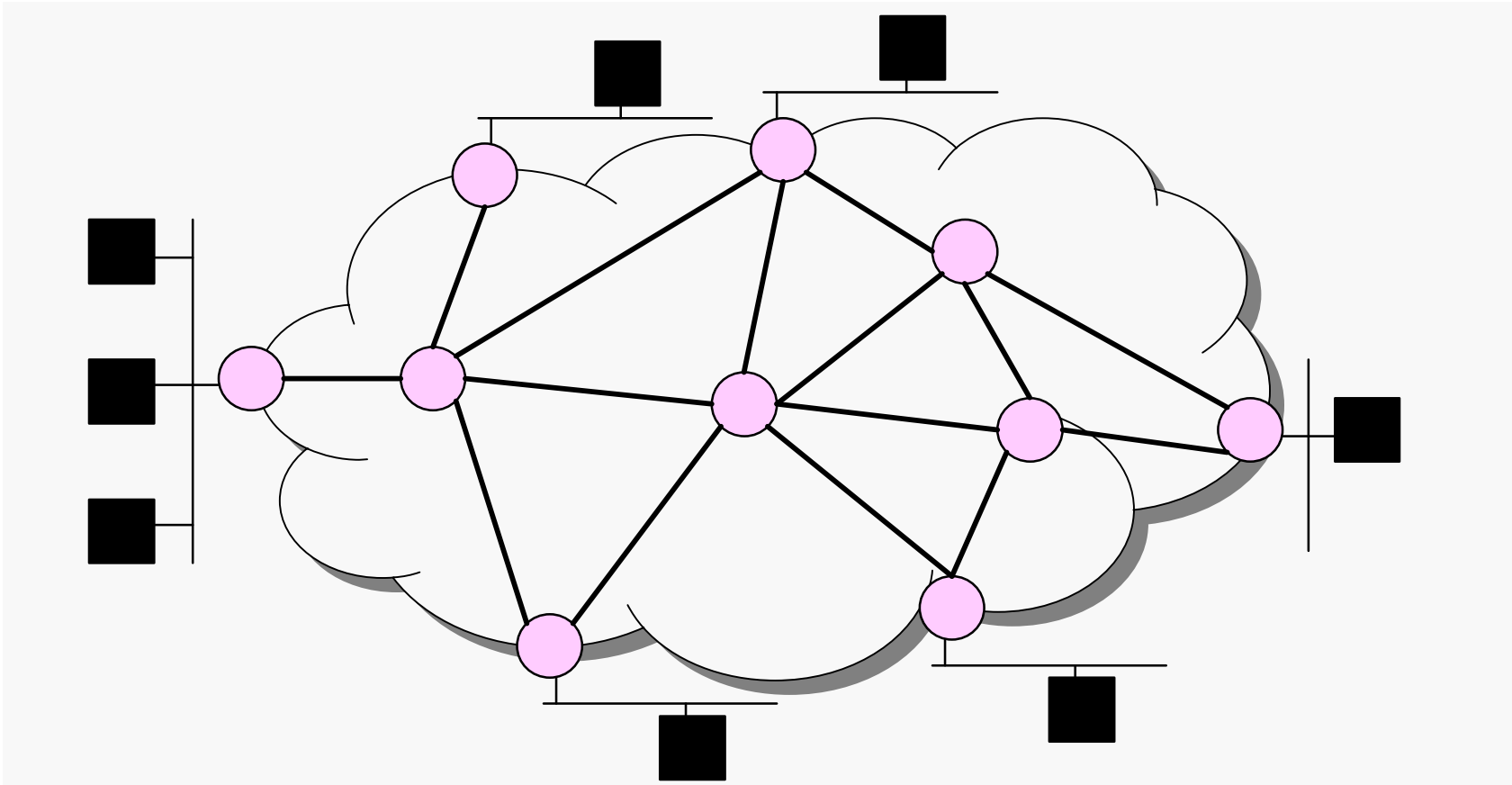


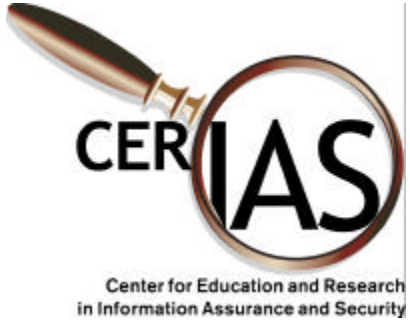
Network Overview

- Two types of network entities
- Hosts
  - PCs, workstations, user oriented
  - On edge of network
- Routers
  - Make up infrastructure
  - Enable communication

Center for Education and Research in Information Assurance and Security

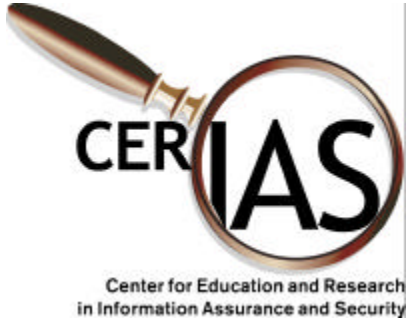
Network Diagram





Communication

- IP networks are packet switched
- Connections between machines are streams of packets
- Hosts create packets and send them into network
- Routers forward to destination

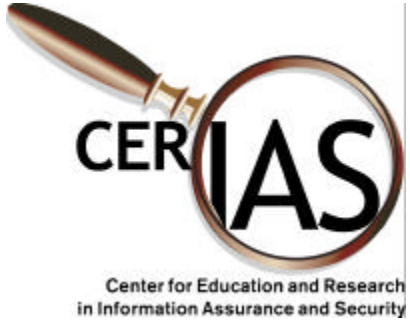


Packets

- Packets have two main parts
- Data
  - Created by and sent between hosts
- Headers
  - Routing information, used for forwarding

    Source Address Destination Address

    Other information

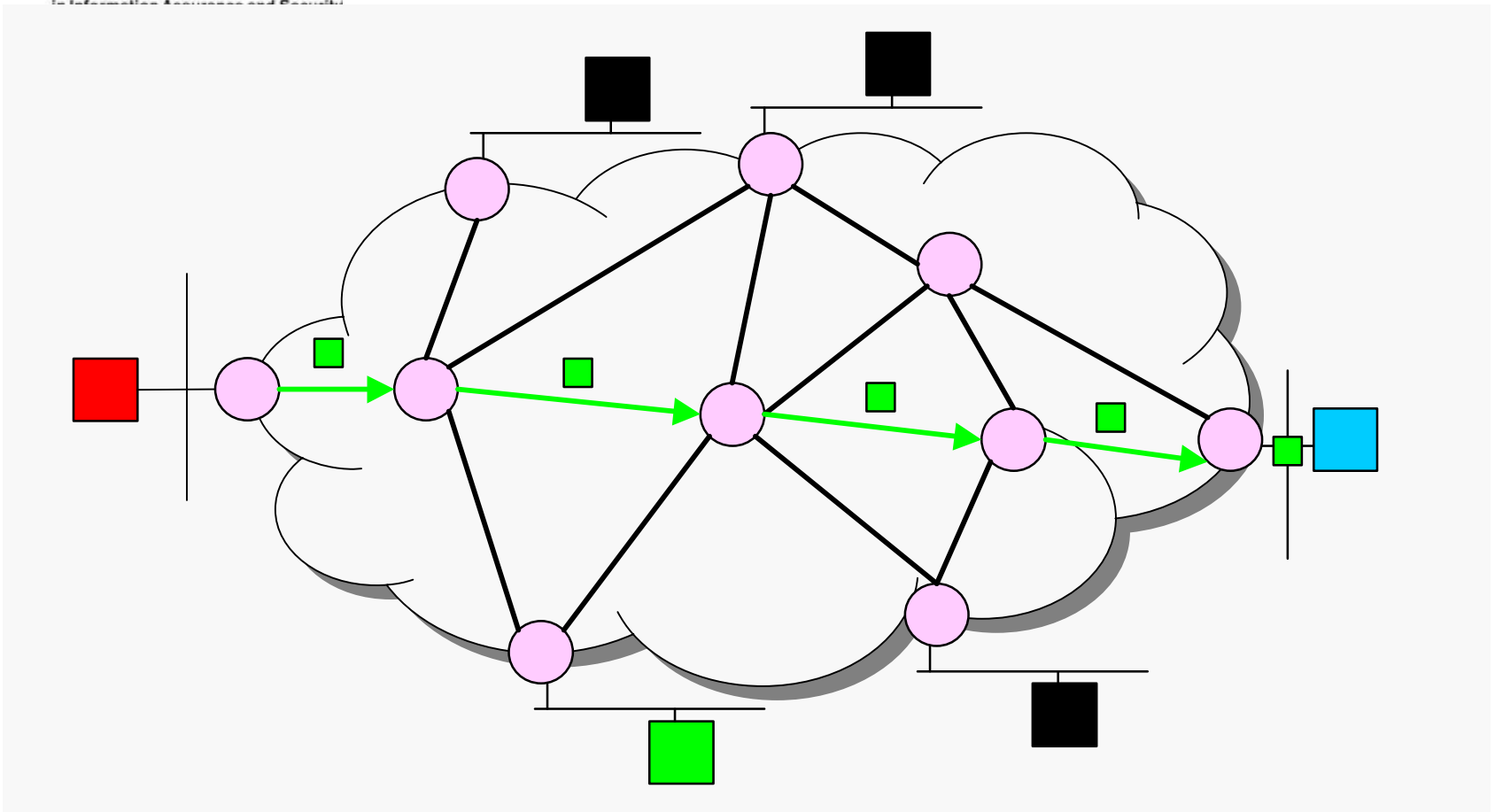


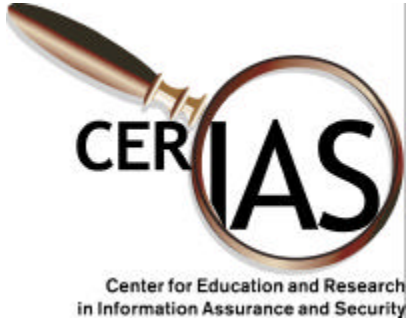
Packet Source Location

- Source addresses in packet headers can be lies
- Routing typically only uses destination address
- Allows construction of packets that appear to be from elsewhere

Center for Education and Research

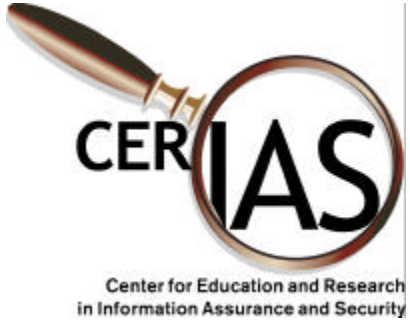
IP Spoofing





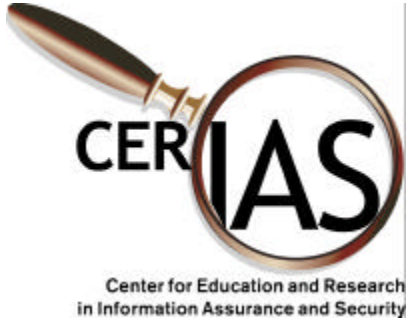
Why is this a problem?

- IP Spoofing
  - Pretend to be another host
  - Exploit address-based trust relationships
- Denial of service attacks
  - Hide source
  - More effective attacks



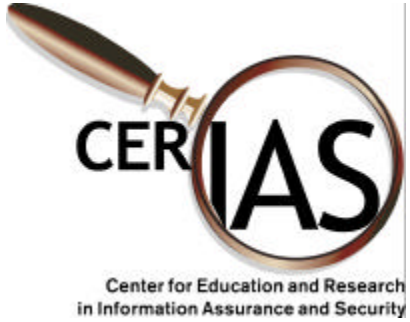
Spoofing Prevention

- Practical measures:
  - Turn on source address routing checks at edge domains
  - Desirable behavior for Internet community
  - Not done frequently enough
  - How frequently done at all is the question



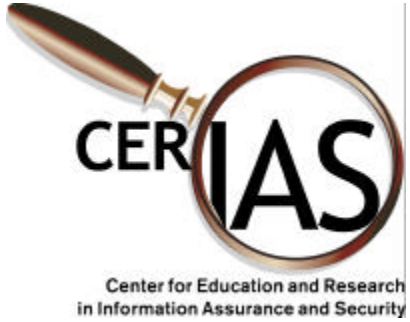
Spoofstat

- Conduct measure of how many domains conduct filtering
- Downloadable client tells what filtering a domain does
- Server keeps statistics on how much filtering occurs
- Encourage good network citizenship



Denial-of-Service Attacks

- Attackers desire to prevent normal network operation
- Various motivations for doing this
- General method is to send packets that cause other communications to fail

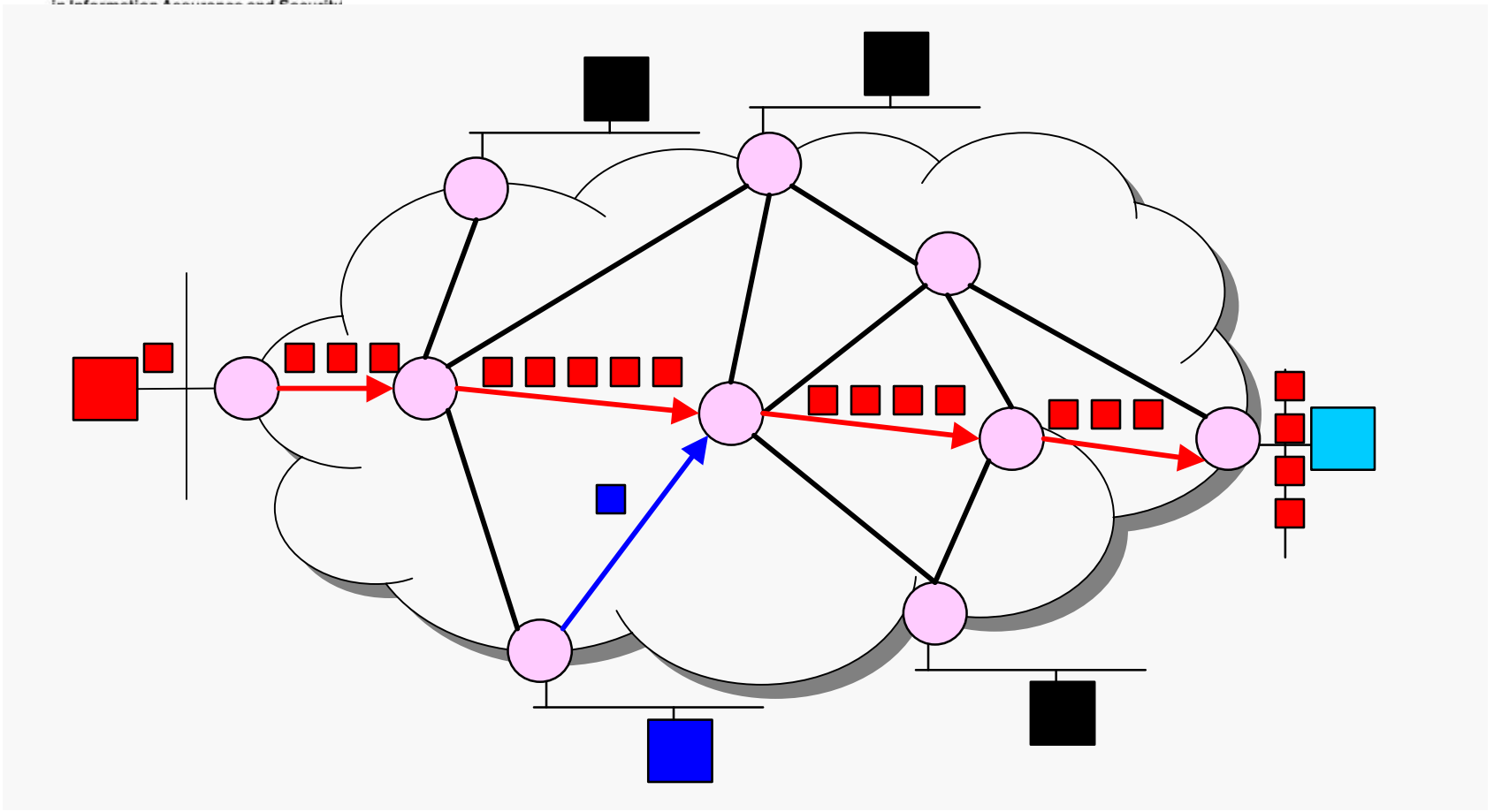


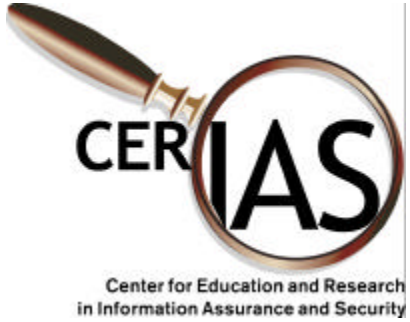
Types of DoS Attacks

- Bug exploitation
  - Send packets that cause buggy TCP/IP stack to crash or hang
- Control Messages
  - Forge network control messages to disrupt network operation
- Flooding
  - Consume resources with massive number of packets

Center for Education and Research

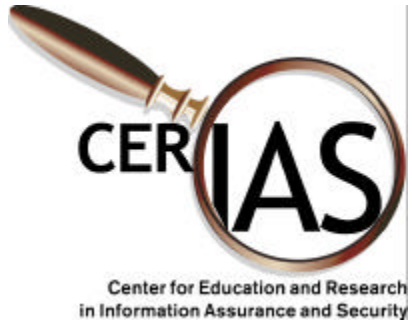
Flooding Attacks





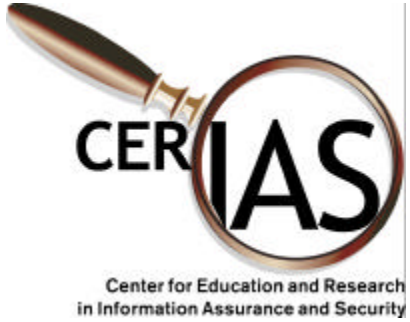
Flooded Packets

- Can consume host resources
  - SYN packets
- Can consume bandwidth
  - Large ICMP or UDP
- Attacks work if attacker can consume enough resources to effect ability of victim to provide service



Distributed Denial of Service

- Attackers with lower bandwidth can't easily flood a victim with higher bandwidth
- Solution for attackers is to find a means of generating more traffic
- Distributed denial-of-service tools
- These attacks were used against Yahoo and others

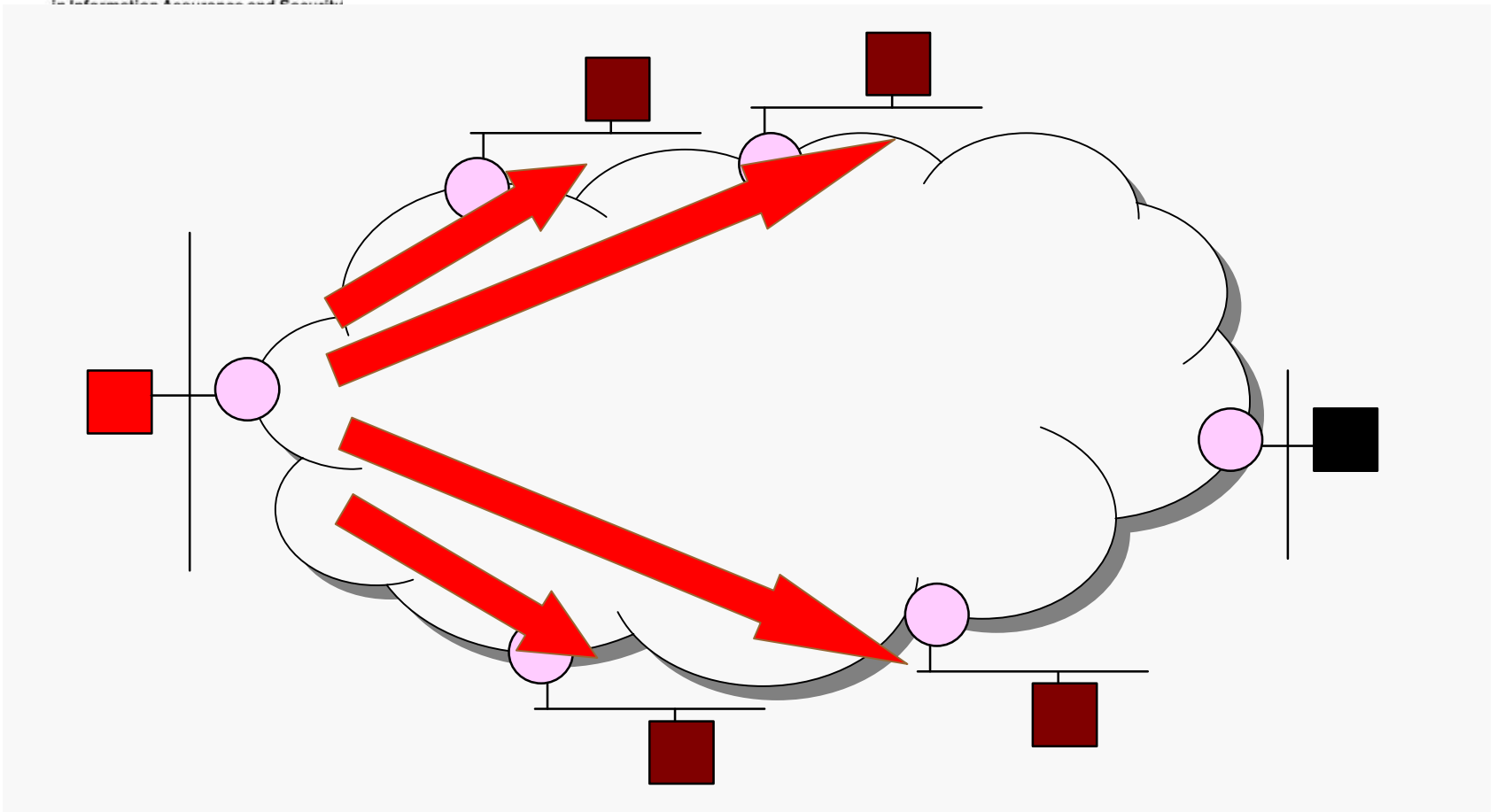


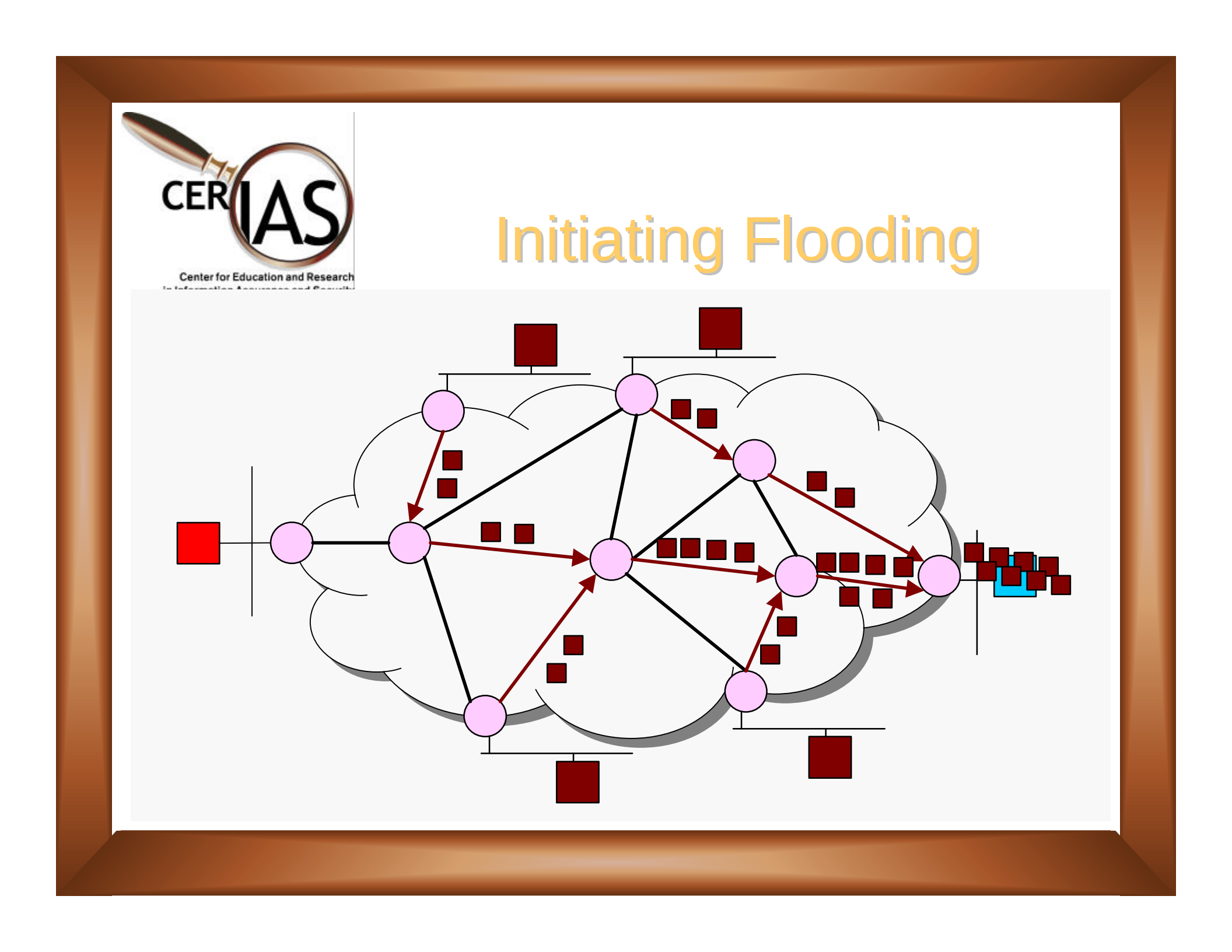
Distributed DoS

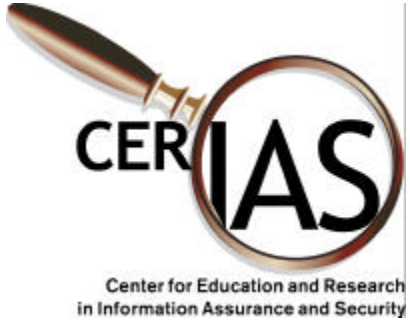
- Attacks work in two rounds
- Attacker exploits vulnerabilities to break into many systems
- Attacker installs software clients
- Master software controls clients to initiate denial of services

CERIAS
Center for Education and Research

Compromising Hosts

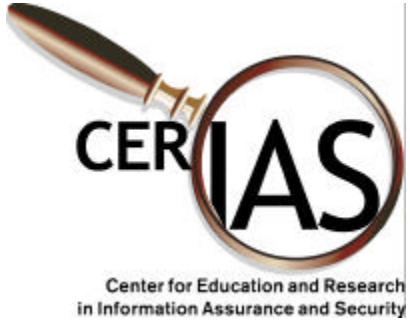



CERIAS
Center for Education and Research
Initiating Flooding



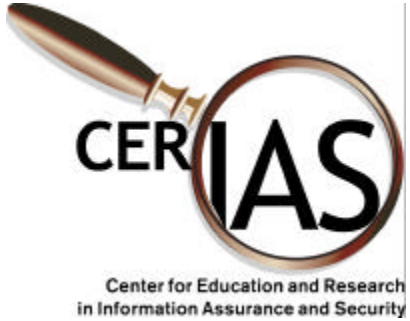
Detecting Denial of Service

- It is not always obvious when a DoS attack is occuring
- Took Yahoo over an hour to determine it was under attack
- Requires system administrators to investigate network outage
- Type of attack is not always immediately evident



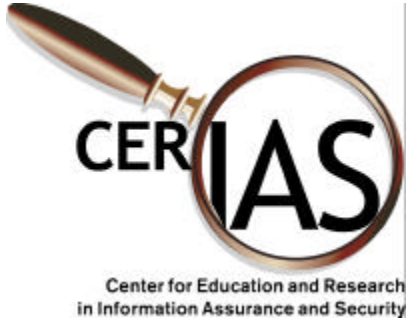
DoS Detection

- Develop tools to determine when DoS occurs and to categorize the type of attack
- Early warning allows rapid response
- Currently gathering data about normal traffic and DoS traffic to train machine learning algorithms



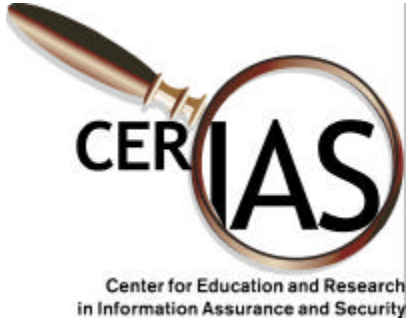
How do you find an attacker?

- Trace flooded packets to the source
- Trace control messages back to master
- Trace attacker back from master to origin of attack
- Easy, right?



Packet Source Location

- Flooded packets are sent with forged IP addresses
- Currently no way to determine source of packet from packet itself

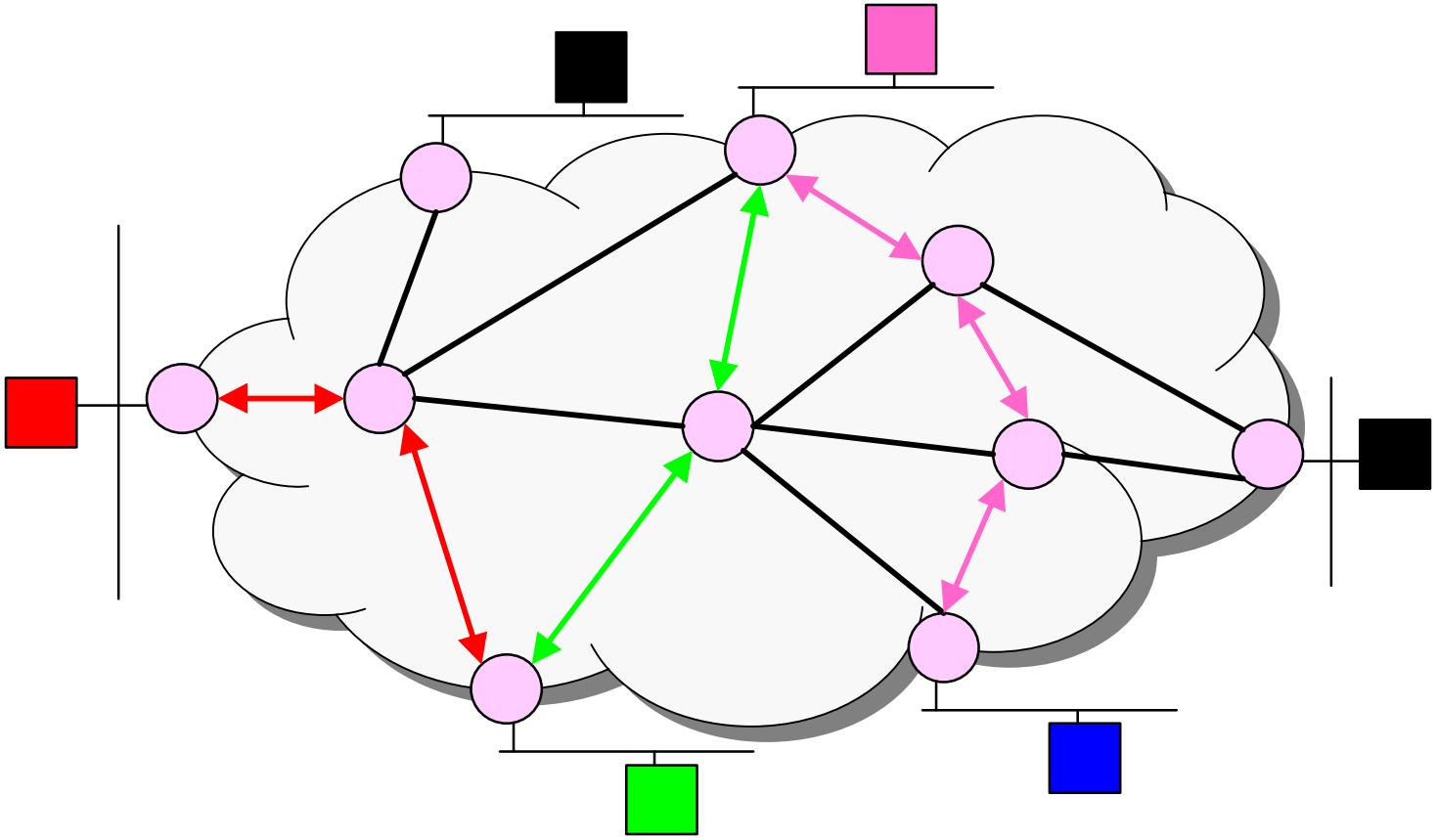


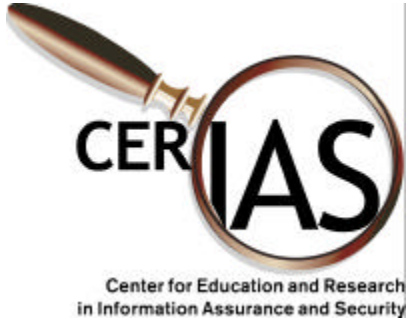
Tracing an Attacker

- If you are able to identify DoS traffic sources and master, need to find origin
- Attackers generally hide by connecting through multiple compromised hosts
- Need to follow TCP stream through network

Center for Education and Research in Information Assurance and Security

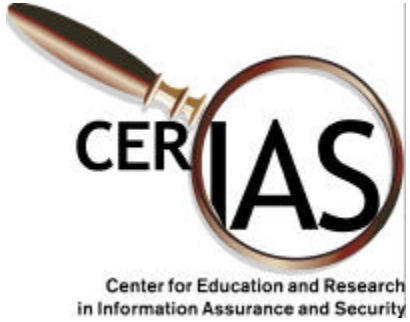
Tracing an Attacker





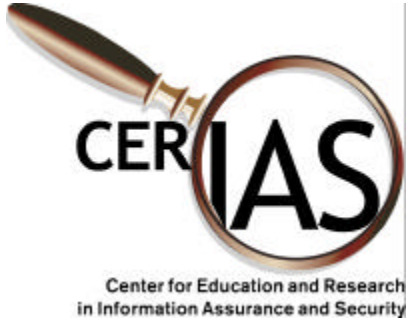
Packet Tracker

- Goals:
  - Stimulate research to solve these problems
  - Produce a workable solution for some environment
- Where we are now:
  - Completed literature review
  - Identified environments and concerns
  - Investigating existing solutions



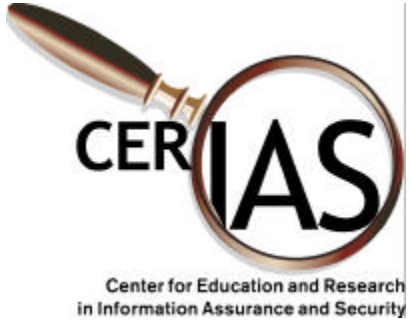
Future Work in Traceback

- Marking of single packets for source determination
- Encrypted stream matching
  - Match encrypted streams based on timing and/or size of packets
  - Method for maintaining audit data about connections
  - Host support for stream traceback



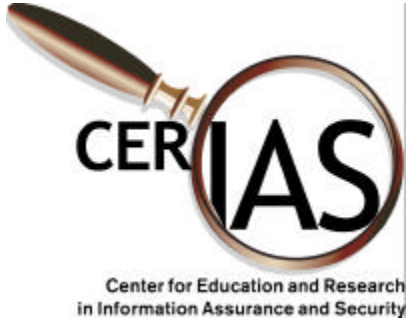
Privacy Concerns

- If traceback solutions are successful, privacy will likely be a concern
- Desirable to have method of maintaining privacy
- Protocols exist to provide network anonymity
- Use same techniques as attackers to hide IP addresses



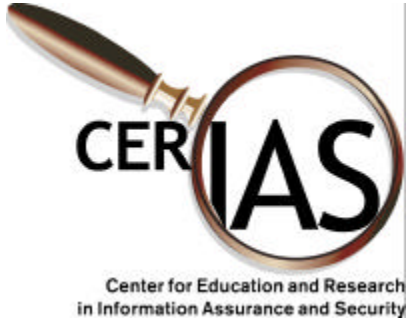
Anonymous Protocols

- Develop anonymous protocols and understand their properties
- Arrive at a logic that describes such protocols
- Useful for privacy
- Also useful for traceback



Hordes

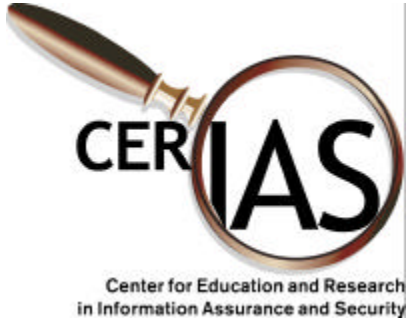
- Work done with Brian Levine, UMass
- New protocol for anonymous communication
- Uses IP multicast for lower communication latency
- Being implemented here
- One of family of protocols being developed



Goals

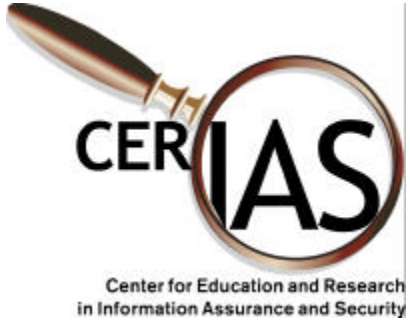
- Eventual goal of my research

The network should provide privacy and anonymity for network users unless they have violated some law, in which case appropriate authorities should be able to rapidly and easily identify suspects



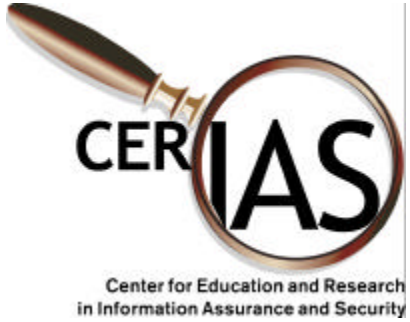
Overview

- Denial of service
- Traceback
  - Encrypted streams in network
- Anonymity



But wait!

- Secure routing
  - Secure Local Area Multicast (SLAM)
    - Enabling technology for IP multicast
    - Source and receiver access control
  - Ant Routing
    - Secure, robust, multi-path routing
    - Based on biological behavior of ants



Contact

clay@cs.purdue.edu