CERIAS

Intrusion Detection System Research Group

Active Group Members

Megan Carney	Benjamin Kuperman
Abhilasha Bhargav	Blake Matheny
William Frauenhofer	Dave Wilson

Goals of the Group

Keep current on IDS research and tools

Share information resources (library)

Work on long term projects

Increase collaboration among students

Increase submissions to conferences

Build software tools

Past Projects

Searchable, online collection of IDS literature

Low and slow scan detection

- Define characteristics of stealthy attacks
- Determine techniques to detect them

Worm Detection (Digging for Worms, Searching for Answers CSAC 2002)

- Analyze and categorize widespread attacks.
- Investigate the life cycle of code propagation to aid detection.

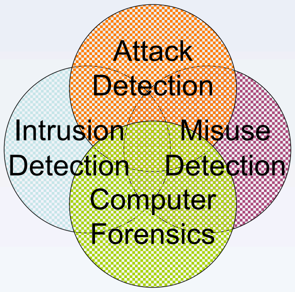
IDS Testing Methodology Improvements (Current Project)

Gaps in IDS Testing:

No current test methodology includes all known useful metrics such as false positives, false negatives, stealthy attacks, etc.

It is unclear how current results apply to specific network environments. Current IDSes have a wide array of monitoring capabilities that fall into specific categories such as attack detection, intrusion detection, misuse detection and computer forensics audit data. A testing methodology should clearly determine how well an IDS performs in each of these categories.

Objective, repeatable usability testing to determine what level of expertise is required to use the IDS effectively.



PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center