Graph-based Intrusion Detection System

February 26, 1997

Steven Cheung
Rick Crawford
Mark Dilger
Jeremy Frank
Jim Hoagland
Stuart Staniford-Chen (co-ordinator)
Steven Templeton
Karl Levitt (PI)
Scott Walnum
Christopher Wee (curmudgeon)
Raymond Yip

The Problem

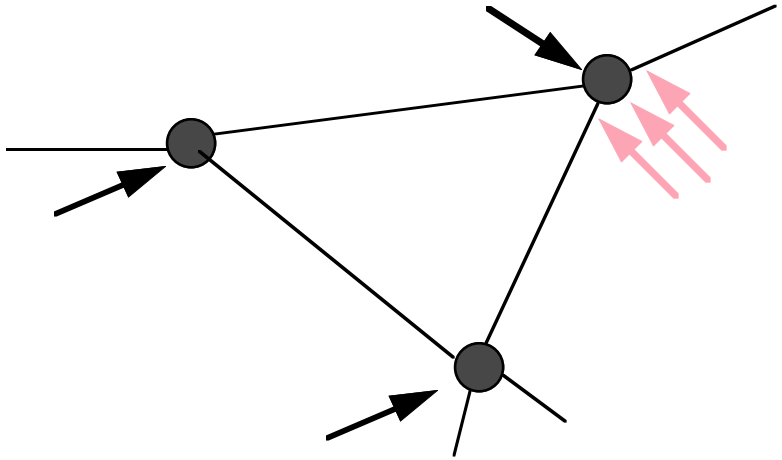
A large organization has many networks and hosts

Centralized IDS does not exploit local knowledge

Centralized IDS does not scale

Department network, hosts & IDS are heterogeneous

Organization is vulnerable to a distributed, coordinated attack



Core ideas

A hierarchy of departments and networks

Graphs abstract network traffic

Graphs propagate up the hierarchy

Engines aggregate graphs

Aggregation and pattern detection in a ruleset

Rulesets are inherited (via hierarchy)

Status of the GrIDS prototype

- Improved stability since last report
- Access control
  - Implemented but not fully tested
- Increased efficiency
  - network was not a bottleneck
  - inefficient networking software was
- Near-real time detection of worms & sweeps
- Memory usage is not optimized
- Deployment in UCD CS network underway

Evaluation by simulation

Prototype has been deployed in lab of 15 hosts

Want to scale to 100's or 1000's of hosts

- Simulate GrIDS traffic to centralized Hierarchy Server
- Simulate user traffic
- Simulate engine aggregation
- Design rulesets to detect traffic
- Measure detection accuracy, precision and latency of detection

Limitations of our prototype

- Fault tolerance
  - Vulnerable to host failures; currently no recovery
  - A congested network may deny service to GrIDS
- Attacks upon GrIDS
  - Unauthenticated; trust required
  - Difficult to securely boot-strap a wide-area IDS
- Quality & quantity of data sources
  - More data sources are needed
  - Our focus aggregation mechanisms, less so on ruleset capabilities

Future work

Short term

- Tolerate single host failures; simple recovery
- Deploy and evaluate within UCD CS department (Feb-June ‘96)
- Seeking partners for larger evaluation (Boeing? Aerospace?)

Long Term

- Simpler means to specify “interesting” graphs (i.e., improved ruleset language, or graphical front-end)
- Hardening of system against attack or exploitation
- Automated response

References

http://seclab.cs.ucdavis.edu/arpa/grids

S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS: A Graph-Based Intrusion Detection System for Large Networks". *Proceedings of the 19th National Information Systems Security Conference*, Oct 22-25, 1996.