Sequoia – A Robust Communication Architecture for Collaborative Security Monitoring Systems

Motivation
Isolated security monitors are often less effective
Collaborative monitors will be more effective by sharing data

Goal and Design Guidelines
A fast, secure, robust and scalable structure of security monitors that supports a rich set of monitor communication patterns

- A two-level communication infrastructure
  - High trust, high performance dominators
  - Low trust, low performance dominees
- Topology-aware neighbor discovery for low latency
- Self-organization for adaptability
- S-certificates for monitor property certification
- Rich communication patterns
  - 1 to 1: unicast
  - 1 to n: dissemination
  - n to 1: subscription
  - m to n: collaboration

Approach
Monitor Neighbor Discovery
- Obtain coordinates & recommended neighbors
- Talk with recommended neighbors
- Establish monitor neighborhood

Distributed Dominator Selection
- Scoped dominator advertisement
- Scoped dominator search
- Handshake between dominator & dominee

Communication Path Discovery
- Two-level communication infrastructure
- Fast & secure routing through hierarchical CAN

Example Information to Share
- Suspicious worm events
- Suspicious DDoS traffic
- Blacklist of misbehaving nodes

Network Research Group
Computer Science Department
University of Oregon
Students: Xun Kang, Dayi Zhou, Dan Rao
PIs: Jun Li, Virginia Lo
{lijun, lo, kangxun, dayizhou, rao}@cs.uoregon.edu
http://netsec.cs.uoregon.edu/research/sequoia.php