Marianas: Survivable Trust for Critical Infrastructure

D. M. Nicol, J. J. Farris

Summary
Explores how peer-to-peer networking among nodes equipped with specialized secure hardware can provide a distributed trusted third party that survives attacks on the networking infrastructure.

Issues we consider include:
- development of peer-to-peer protocols tailored to trust models
- development of applications for these capabilities
- modeling and simulation of large-scale Marianas systems to evaluate the effectiveness of the techniques

Recent and future work:
- Evaluation of secure peer-to-peer routing overlay networks for SCADA systems
- Peer-to-peer trust protocol
- Scalability of trust protocols

Example: SCADA Systems
Supervisory Control And Data Acquisition (SCADA) systems gather and analyze data for real-time control and are used extensively, in applications such as electrical power distribution, telecommunications, and energy refining.

For our simulations, when it appears that real-time message delivery constraints are not being met (due, for example, to a denial of service attack), a peer-to-peer overlay network is used to route message floods in an effort to ensure delivery. The SCADA system, and peer-to-peer nodes all use strong hardware-based authentication techniques to prevent injection of false data or commands, and to harden the routing overlay.

Model:
- Delivery of sensor messages to the master station
- 20 interconnected LAN networks
- Over 1000 interconnected active devices
- DDoS bandwidth consumption attack on selected network paths

Concept
Peer-to-peer Networking
Increase survivability to network infrastructure attacks through use of peer-to-peer overlay network

Properties:
- Each node acts as client and server
- Unstructured peer-to-peer network (e.g. Gnutella)
- Message routing via controlled flooding over UDP
- No use of ‘super-node’ or ‘ultra-peers’ in order to limit impact of node loss

Simulation Results
Our simulations using the SSFNet network simulation framework help to quantify the anticipated tradeoffs of message survivability and latency minimization. We compare model SCADA systems using only a traditional communications model versus one including a backup peer-to-peer overlay.

Results:
- Higher on-time message delivery with overlay
  - see graph below
- Higher average message latency with overlay
- Higher average number of message hops with overlay

Specialized Secure Hardware
Establish trust relationships and secure communications channels through use of remote attestation and specialized secure hardware (e.g. TCG/LaGrande).

Properties:
- Remotely attest to hardware, OS, and application through validation of signed nested public key certificates
- Allow detection of tampered or corrupted components on remote hosts
- Enhanced authentication for hosts joining peer-to-peer network

Future Directions
Peer-to-peer trust protocol
- securely handle node joins and leaves from peer-to-peer network
- tailored to trust model through inclusion of remote attestation
- DDoS protection through specialized client puzzles

Scalability of trust protocol
- Securely load-balance join requests to existing nodes
- Specialized entry nodes redirect new joiners to available existing nodes
- Build lists of available nodes through ‘crawling’ peer-to-peer network similar to web search engine spider