A Proposed ABone Network Security Architecture

Bob Braden
Bob Lindell
Steven Berson
USC/ISI
Goals

- Provide initial ABone security capabilities
- Propose a flexible framework
  - With room to grow
  - Incorporate future research results
- Make the ABone security architecture draft a living document
AAs and Activities

- **AA**
  - Active Application code
  - Some can concurrently process multiple activities

- **Activity**
  - Executes in an AA on behalf of a particular end user or "principal"
  - Involves data communication along the path(s) between senders and receivers
  - Active processing or computation within both hosts and routers
ABone Node Security

- Unix Operating System
  - Separate user identity for each EE
  - Network traffic control implementation
- Anetd
  - Secure EE invocation
- QCMD
  - Secure distribution of ACL and policy information
ABone Network Security

- Considerably more challenging
- End-to-end security with hop-by-hop packet modification
Threat Model

- Activity denial of service (node security issue)
- Unauthorized use of resources
- Malicious modification of packets
- Injection of spoofed packets
- Replays of previously transmitted packets
Trust Model

- Some AAs assume complete trust in the network. Any solution MUST offer a low overhead solution for these AAs.

- Some AAs may trust nodes but not the communications infrastructure that comprises the network.

- Some AAs may not even trust the nodes. By definition this implies an AA–based solution.
Proposed Solution

- User authorization to decide if the principal is authorized to launch this activity, obtain special resources, and determine how to account for the services

- Message authentication and integrity to ensure that control and data packets for the activity cannot be spoofed, modified, or replayed
User Authorization

- Packets carry a certificate, not generally modified at each hop, that is disseminated end–to–end
- Likely to be rewritten at provider boundaries in a multi–provider network
- AAs may wish to bind this certificate to invariant portions of the message to prevent misuse (no node trust)
- User authorization ("Policy") is an active area in IETF. Can we leverage off their work?
Message Authentication and Integrity

- Packet carry an outer keyed hash and sequence number to prevent modifications and replays.
- For persistent AAs (not capsules), packets carry an inner hash identifying the sending AA. This is a dynamic naming convention used to isolate activities.
- This "iterative" trust model provides the necessary scalability needed in active networks.
- Assumes a homogeneous level of trust along a path.
Secure Node Operation

- Maintain node security
- Preserve secrets
- Peer only with other trusted nodes
- Reject all messages which cannot be properly authenticated using the outer keyed hash
- Reject all messages which do not carry a correct inner hash for a given activity
- Place a proper inner hash, based on the sending AA, into outgoing packets.
User Identity

- Principals launch activities at end nodes
- Must provide a scalable solution
- Common case is the initiation of an activity within a single domain of trust
- User identity could be carried in the authorization certificate and be based on server technologies such as Kerberos
Recovery

- We have assumed node security
- What if a node was compromised?
- Iterative trust implies we must recover all nodes in the network?
- Solutions when this is inadequate
  - Robust activities
  - Compartmentalized network
Future Directions

- Robust Activities
- Policy Definitions
- Mobility
- Supply requirements for future NodeOS and EE draft security specifications