Secure Local Area Multicast
SLAM

Clay Shields
Christopher Adam Telfer
IP Multicast

• There are 3 types of Internet traffic

• Unicast – one to one
  - a telephone call

• Broadcast – one to all
  - a PA announcement

• Multicast – many to many
  - a conference call
Slow Adoption of IP Multicast

- IP multicast provides efficient multi-party communication
- Particularly useful for streaming video
- No source access control allows anyone to send
- No receiver access control allows anyone to receive
SLAM : Secure Local Area Multicast Routing

Centralized Multicast

+ Proxy for Sender Access Control

+ Encryption for Receiver Access Control

= SLAM
SLAM : Sender Access Control

- All multicast traffic which is subscribed to within a domain goes to a proxy
- Proxy retransmits data to subscribed receivers via multicast
- Local multicast routing is set up by the centralized controller
- Incoming traffic may be controlled via the proxies
SLAM: Centralized Multicast Routing

• 1+ web servers handle requests for multicast traffic (and billing)
• Web servers issue confirmed requests to a central controller
• Controller changes routing entries directly on routers
• Controller communication with routers is encrypted and authenticated
SLAM : Receiver Access Control

• Proxies encrypt traffic to local receivers.
• Key schedule for encryption is determined in advance.
• Subscribing hosts receive a portion of the key schedule from the web server.
• Subscribers only receive keys for the duration they have paid for.
SLAM : Implementation

• SLAM is implemented in FreeBSD

• Each FreeBSD box can act as a router

• One machine in the network should run the controller daemon

• A network may support multiple proxies
SLAM : Future Work

• Add a GUI for management
• Create more configurable proxies
• Create web interface for control
• Use SNMPv3 for control of routers
SLAM : Subscription Phase

Key
1 - Subscribe
2 - Key Schedule

R - Router  C - Controller  S - Subscriber

P - Proxy
SLAM: Routing Phase

Key
1 – Multicast Routing Changes

R – Router  C – Controller  Active Link
P – Proxy  S – Subscriber
SLAM: Traffic Phase

**Key**
1. Incoming Multicast Traffic
2. Encrypted Multicast Traffic

**Legend**
- R: Router
- C: Controller
- P: Proxy
- S: Subscriber
- Active Link

This EPS picture will print to a PostScript printer, but not to other types of printers.