IRTF GSEC meeting

Pete Dinsmore

Lakshminath R. Dondeti

IETF-56

March 18 2003, San Francisco

Agenda

- **Review of charter and future directions**
  - Pete and Lakshminath … **15 mins**
- **A Simple Stream-Authentication Scheme**
  - Hovav Shacham … **30 mins**
  - joint work with Eu-Jin Goh and Nagendra Modadugu
- **Review of recent work on multicast security**
  - Lakshminath … **15 mins**

Review of GSEC Charter

- **Security issues of large and small groups**
- **Broadcast, multicast and anycast security**
- **Groups that may (not) use multicast**
- **Stability and convergence of group security protocols**
  - Group size
  - Membership dynamics
  - Topology
  - Bandwidth constraints
  - Centralized / distributed control etc.

GSEC Charter … continued

- **Examples of areas of interest**
  - Group policy management
  - Decentralized group key management
  - Closed and open group security
  - Multi-sender group security
  - Membership management
  - Security protocols for groups other than mcast
    - Unicast and Anycast
  - Traitor tracing

GSEC: goals

- Review of past and current work
- Evaluation of available technologies
- Development of new technologies
- Identification of technologies ready for standardization

Future directions

- **Active collaboration with MSEC**
- **Pre-Standards work on existing technologies and transition to MSEC**
  - e.g. MESP I-D specifies RSA and TESLA as source authentication options
  - There are others that need to be standardized
  - GSEC can be a forum for discussions
- **MSEC charter (being) revised**
  - Watch for new topics there