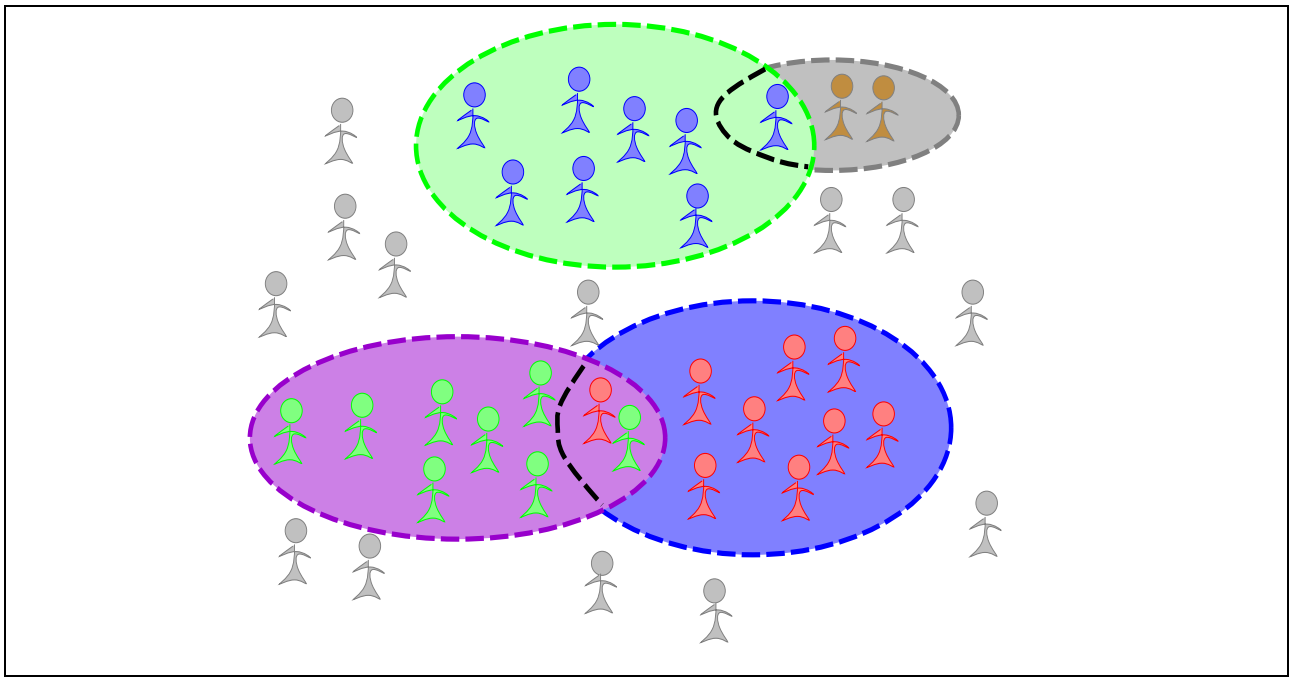
CLIQUES : Security Services for Group Communication

GENE TSUDIK
USC Information Sciences Institute
Marina del Rey, CA
gts@isi.edu



..... *CLIQUES* Motivation .....

Group communication occurs in many settings: from low-level network multicasting to tele- and video-conferencing.

Examples:

LOTUS NOTES, OSPF, RSVP, MUDs, GLOBUS, MBONE apps., etc.

Secure group communication is:

- **Crucial** in military and law enforcement operations
- **Necessary** in commercial and public sector environments

What is the problem?

- Peer-to-peer security is well-understood
- Secure group communication is relatively unexplored.
- Lack of a general-purpose group security solution
- Typical security services: communication privacy and integrity.
- Not possible without secure and efficient **key distribution**, authentication and other mechanisms.

..... *CLIQUES* project goals .....

1. **Analyze** security requirements of group communication
2. **Design** a suite of key distribution, authentication and other protocols
3. **Realize** them in a general-purpose toolkit
4. **Address** challenges of latency, state and scale
5. **Demonstrate** results in different application domains

.....Design principles .....

- Support **dynamic group membership**
  operations at granularity of individual members and entire subgroups
- Provide **scalable** and **flexible** services.
  All sizes and compositions to be accommodated. No reliance on network topology or communication paradigm.
- Support **highly secure** operation.
- Strive for **near-optimal efficiency.**
  minimize latency, bandwidth and state retention. Many performance factors to be considered.

Additional factors to take into account:

- low-bandwidth (e.g., wireless) communication
- user/device mobility
- low-power, low-storage devices
- export regulations
- real time constraints

. . . . . Starting point . . . . . .

M. Steiner, G. Tsudik and M. Waidner
"Diffie-Hellman Key Distribution Extended to Groups"
1996 ACM Conference on Computer and Communications Security,
March 1996.

- Defined a class of *natural* Diffie-Hellman extensions
- Proven security of the entire class
- Developed 3 extensions to n-party case
- Evaluated/analyzed efficiency factors

. . . . . Related work . . . . . .

Practical:

- ISAKMP, Photuris, Oakley
- ISIS/CHORUS
- IOLUS

Crypto:

- Burmeister/Desmedt (UWM)
- Steer et al. (BNR)
- Just (Carleton)
- Ingemarsson et al. (???)