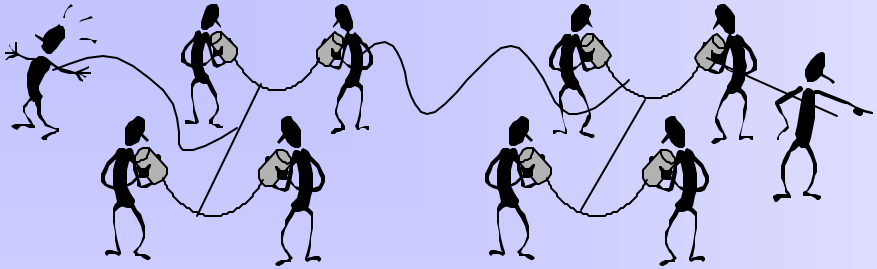
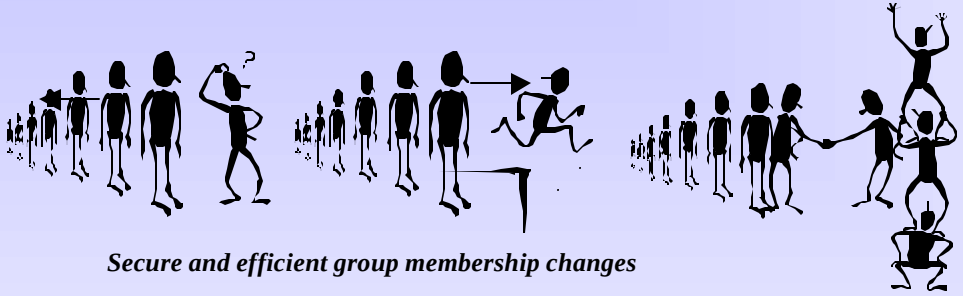
CLIQUES: security services for dynamic peer groups



Decentralized authenticated group key agreement with provable security



Secure and efficient group membership changes

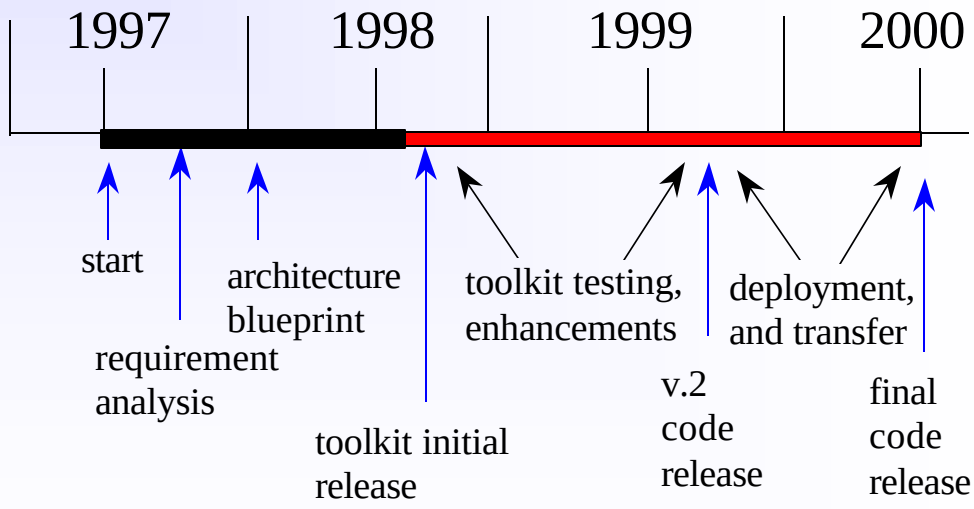
New Ideas

- Efficient and provably secure authenticated group key agreement techniques. New security services, e.g., group integrity. Efficient group signature scheme.
- Contributory cryptographic protocols geared towards dynamic peer groups irrespective of underlying communication paradigm, protocol layer and network topology.
- Systematic approach to protocol performance evaluation including consideration of new protocol complexity and efficiency metrics.

Impact

- λ Versatile and flexible CLIQUES toolkit and API offering security services for dynamic peer groups.
- λ Security services for replicated server groups, groupwork applications, multi-user games and simulations.
- λ Understanding of DPG security requirements, corresponding mechanisms and efficiency/performance metrics.

Schedule



USC / Information Sciences Institute: Gene Tsudik