The Private Peer Sampling Service
The Ground for your Secret Society

Valerio Schiavoni, Étienne Rivière, Pascal Felber

University of Neuchâtel, Switzerland

Context and Problem

- Large-scale network, no PKS or trusted parties
- Secured communications and confidential membership among members of private groups

Peer Sampling Service: a Building Block for Large-Scale Applications

- Group membership
- Randomness
- Keeps network connected

Continuous stream of alive random nodes at each node

Real World Setting

- NATs
- Firewall
- Relays

Relay nodes

- Help with NATs
- Threat to privacy

- How to use relays but hide source/destination/content?

Group Management

- Creation and admission via signed group keys, passports
- Access via explicit invites (IM, emails, ..)

Private Membership Management

- Gossip-based views exchange
- No direct communications
- PSS over Secure Anonymizing Channels

Private Peer Sampling

- group members
- onion hops

Relay nodes

- benevolent relays
- malicious relays

Onion Views

- Messages exchanged via onion routes
- Decentralized PKI
- Routing challenges:
  - Pub-to-NAT
  - NAT-to-NAT
- Bandwidth cost to maintain onion-friendly views:

Ongoing Evaluation

- Detection/recovery from faulty onion-routes under continuous churn conditions
- Impact of onion-friendly views on clustering
- Computing cost breakdown at relay nodes
- Deployment over PlanetLab and home devices

Implementation

- Tested and implemented using SPLA\* (NSDI'09)
- Lua-based DSL and libraries

www.splay-project.org

---

Private Peer Sampling Service: a Building Block for Large-Scale Applications

- Group membership
- Randomness
- Keeps network connected

Real World Setting

- NATs
- Firewall
- Relays

Relay nodes

- Help with NATs
- Threat to privacy

- How to use relays but hide source/destination/content?

Group Management

- Creation and admission via signed group keys, passports
- Access via explicit invites (IM, emails, ..)

Private Membership Management

- Gossip-based views exchange
- No direct communications
- PSS over Secure Anonymizing Channels

Private Peer Sampling

- group members
- onion hops

Relay nodes

- benevolent relays
- malicious relays

Onion Views

- Messages exchanged via onion routes
- Decentralized PKI
- Routing challenges:
  - Pub-to-NAT
  - NAT-to-NAT
- Bandwidth cost to maintain onion-friendly views:

Ongoing Evaluation

- Detection/recovery from faulty onion-routes under continuous churn conditions
- Impact of onion-friendly views on clustering
- Computing cost breakdown at relay nodes
- Deployment over PlanetLab and home devices

Implementation

- Tested and implemented using SPLA\* (NSDI'09)
- Lua-based DSL and libraries

www.splay-project.org