

Motivation

The deployment of virtual organizations requires significant administration in order to establish and maintain trust, and manage computational resources across multiple organizations. This management overhead has often presented a barrier for collaboration across different organizations. We propose the SocialVPN, a social virtual private network that integrates social networking, and self-configuring peer-to-peer overlay networks to allow for self-managing virtual organizations

Approach

The key principles of our approach:

- Social networking systems (i.e. Facebook) provide base for trust relationships needed for ad-hoc virtual organizations
- Established connections can be mapped to TCP/IP layer for collaboration and resource sharing
- By leveraging IP-based service discovery mechanisms through the Zeroconf/multicast DNS protocol, users can efficiently advertise their services
- Integrating components allows for a self-configuring deployment of collaborative cyberinfrastructures by non-experts

Use case scenarios:

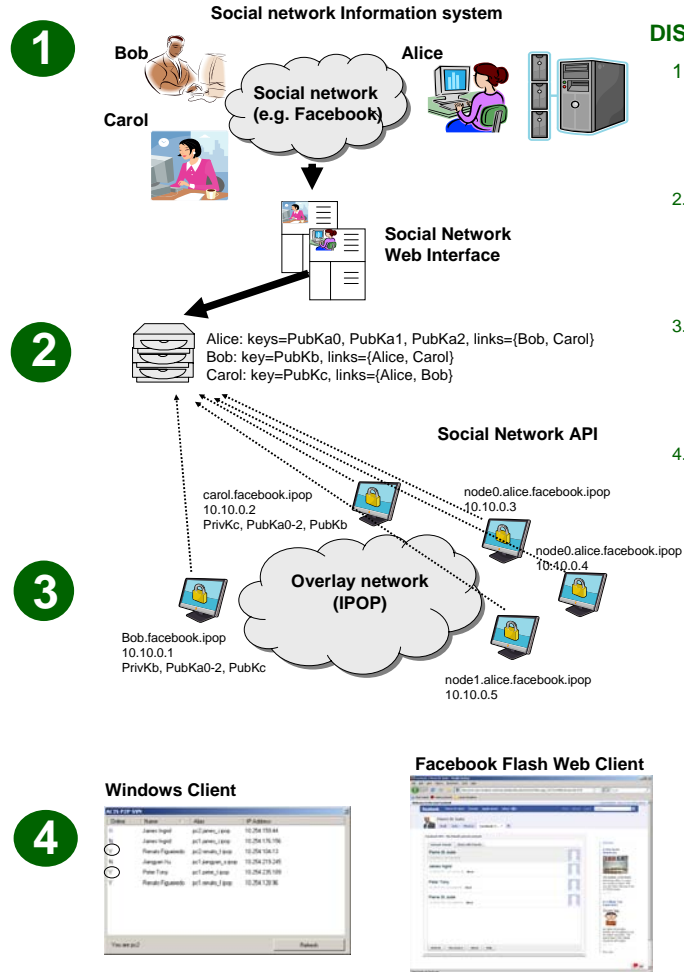
- Ad-hoc Social VPN for collaboration among individuals
 - Remote desktop sharing (VNC, RDP)
 - File sharing (SMB, HTTP, SFTP)
 - Media streaming, VoIP (Ekiga)
- Ad-hoc cycle sharing
 - Condor pools
- Bootstrapping certificate authorities
 - Social network groups

Social Network Integration

We provide a simple REST-like HTTP interface for the following reasons:

- Allow developers to create social networking components that connect users from their preferred social network
- We created a Flash/ActionScript-based client that runs within the browser in a user's Facebook profile
- We are currently working on an OpenSocial web-client which will provide support for other social networks such as MySpace, Orkut, LinkedIn, etc...
- Organizations can use their own social infrastructure to enable these ad-hoc virtual organizations
- SocialVPN application can connect users from multiple social networks simultaneously
- Web-based clients provide more portability across different operating systems

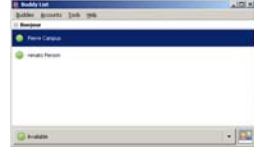
Architecture



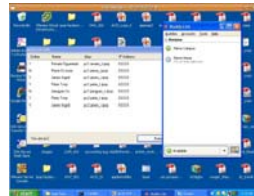
DISCOVERY PROCESS:

1. Alice, Bob, Carol use a social networking website (e.g. Facebook) to establish a relationship
2. VPN application accesses social network database to discover peers and publish/download certificates
3. DNS names and IP addresses are automatically generated, users not required to remember IP addresses
4. Applications/services are discovered through mDNS/SD, a service discovery system implemented by various OSES

Bonjour: automatic discovery



Desktop sharing: VNC/RDP



Virtual Private Network Management

We also developed a system which uses social networking groups to manage an IPSec-based virtual private network:

- Users join a social networking group
- The group creator serves as the certificate authority, and stores a CA certificate in the social networking group datastore
- Group members are able to retrieve the CA certificate from the social networking datastore
- Group members make certificate requests putting them in the social networking datastore
- CA checks social networking and signs requests from group members
- Group members retrieve certificate from social network and uses it for IPSec communication over the virtual network

Future Work

Our long term goals involve creating a self-organizing, self-configuring, and self-optimizing virtual network:

- Efficient broadcasting – use social networking data about users to broadcast a message to all users with the least amount of Internet traffic
- Access control – provide different levels of access to services based on user trust ranking
- Traffic optimization/prioritization – higher ranked users get faster response, schedule algorithm applied to network traffic

References:

- "On the Use of Social Networking Groups for Automatic Configuration of Virtual Grid Environments" in International Workshop on Grid Computing Environments 2008