
On the Use of Social Networking Groups for Autonomic Configuration of Virtual Grid Environments

International Workshop Grid Computing Environments 2008

Pierre St Juste^{*}, David Wolinsky^{*}, Jiangyan Xu^{*}, Michael Covington^{**}, Renato Figueiredo^{*}

^{*}Center for Autonomic Computing, University of Florida

^{**}Corporate Technology Group, Intel Corporation

November 16, 2008

The Challenge

- Common Barrier to Grid Collaboration
 - Group of researchers wants to collaborate
 - Secure access to each other's systems (i.e. Grid resources)
 - Most security models depend on certificates (X.509 and PKI)
 - **End users are not often familiar with security concepts and configuration underlying PKI**
- Complexities of PKI-based systems
 - Certificate Authority (CA) regulates certificate signing
 - CA properly identifies certificate owner
 - Secure distribution of CA certificate
 - CA updates revocation list
 - **Tools for managing groups and PKI over time are not user-friendly**

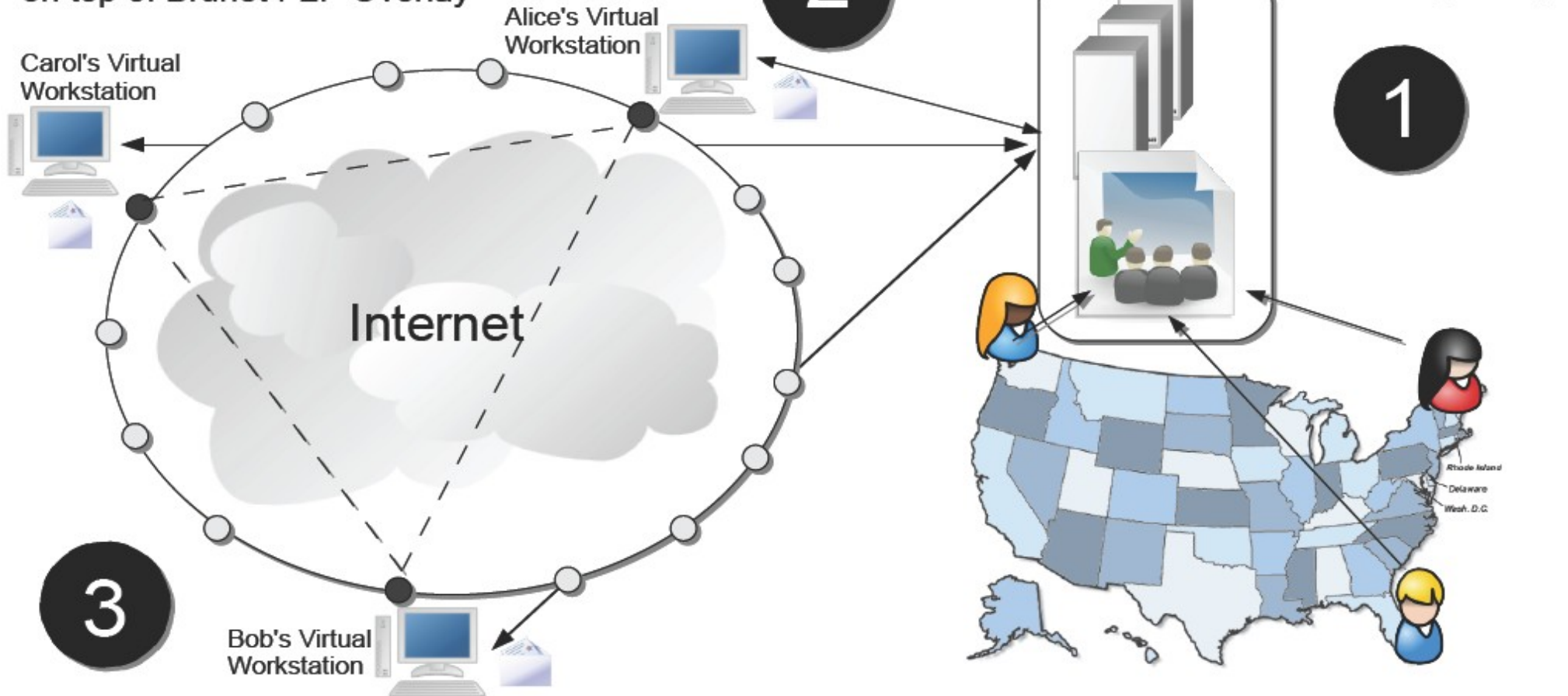
Our Approach

- Use Web 2.0 (social networks)
 - Integrate the management of certificates with social networking groups
- Why social networks?
 - User friendly, intuitive
 - Much easier to manage a social networking group
 - Access through REST API
- **We use Facebook groups to automate certificate signing for IPsec to enable a virtual private network**

The screenshot shows a Facebook group page for 'SecureGridNet'. The page is titled 'SecureGridNet' and is categorized as 'Global'. The 'Basic Info' section indicates it is a 'Student Groups - Academic Groups' with the description 'This is a test group for social network project'. The 'Members' section shows two members: Peter Tony and James Ingrid. The 'Discussion Board' section is empty, with a message 'There are no discussions. Start the first topic.' The 'The Wall' section is also empty, with a text input field and a 'Post' button. The 'Photos' section is empty, with a message 'No one has uploaded any photos. Add Photos.' The right sidebar contains various group management options such as 'Message All Members', 'Edit Group', 'Edit Members', 'Edit Group Officers', 'Invite People to Join', 'Create Related Event', and 'Leave Group'. It also includes a 'Share' button and a 'Group Type' section indicating it is a closed group. The 'Admins' section lists James Ingrid as the creator. The 'Events' section is empty, with a 'Create Events' button. The 'Related Groups' section lists several other groups, including 'Facebook Social VPN', 'Student Groups - Academic Groups', 'Archer community', and 'Internet & Technology - Computers & Hardware'.

Overview

IPOP Virtual Private Network
on top of Brunet P2P Overlay

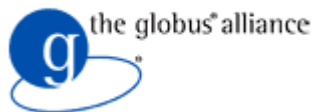


Presentation Outline

- Background
 - Web-based social networking (WBSN)
 - Grid infrastructure: Grid appliance, IPOP virtual private network
- Design Overview
 - Certificate management
- Implementation Details
- Experiments and analysis
 - Ease of deployment, network performance
 - Social Network API Limitations
- Related Work
- Conclusion

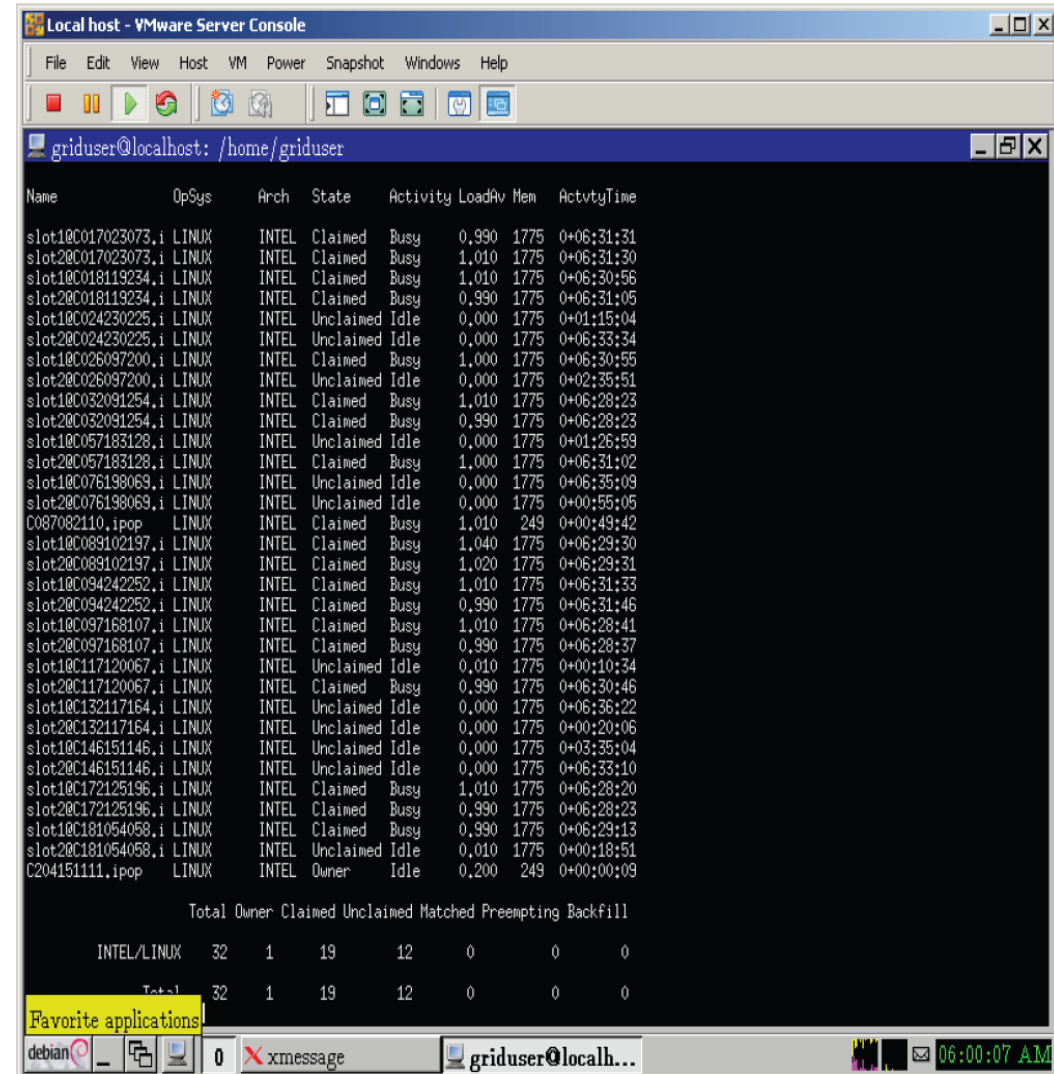
Web-based Social Networking

- Popularity and API
 - Hundreds of millions of users
 - Emergence of social networking applications
 - Facebook Platform API and OpenSocial
- Long-term focus
 - Leverage social networks to build more intuitive systems
 - Design systems with social aspects of users in mind
- **We leverage WBSN technologies to configure Grid environments**



The Grid Appliance Project

- Ease of deployment
 - Prepackaged virtual machine
 - Condor job scheduler
 - Homogeneous software stack
- Desktop Grid
 - End users contribute their desktop to pool of resources
 - **Virtual LAN connects virtual machines**
 - Unmodified applications can communicate (NFS, SSH)
- www.grid-appliance.org



```
Local host - VMware Server Console
File Edit View Host VM Power Snapshot Windows Help
griduser@localhost: /home/griduser

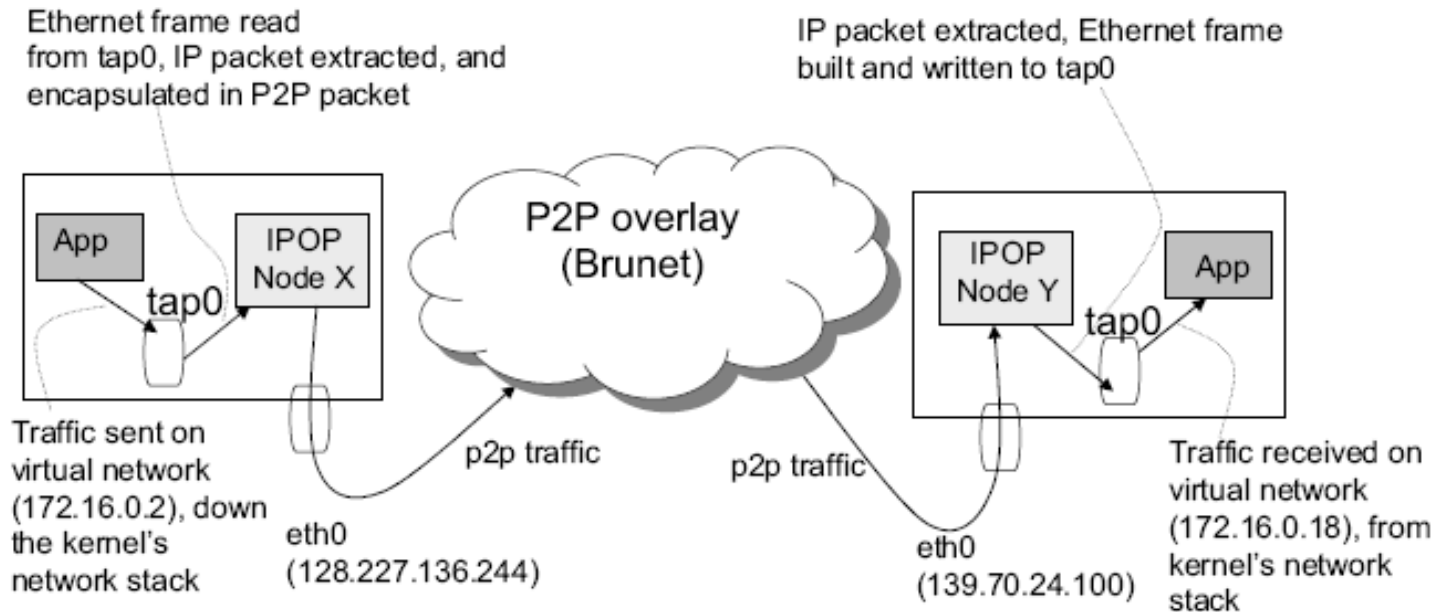
Name      OpSys  Arch  State  Activity LoadAv Mem  ActvtyTime
slot10C017023073,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:31:31
slot20C017023073,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:31:30
slot10C018119234,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:30:56
slot20C018119234,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:31:05
slot10C024230225,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+01:15:04
slot20C024230225,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+06:33:34
slot10C026097200,i  LINUX  INTEL  Claimed  Busy    1,000 1775 0+06:30:55
slot20C026097200,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+02:35:51
slot10C032091254,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:28:23
slot20C032091254,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:28:23
slot10C057183128,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+01:26:59
slot20C057183128,i  LINUX  INTEL  Claimed  Busy    1,000 1775 0+06:31:02
slot10C076198069,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+06:35:09
slot20C076198069,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+00:55:05
C087082110.ipop    LINUX  INTEL  Claimed  Busy    1,010 249  0+00:49:42
slot10C089102197,i  LINUX  INTEL  Claimed  Busy    1,040 1775 0+06:29:30
slot20C089102197,i  LINUX  INTEL  Claimed  Busy    1,020 1775 0+06:29:31
slot10C094242252,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:31:33
slot20C094242252,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:31:46
slot10C097168107,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:28:41
slot20C097168107,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:28:37
slot10C117120067,i  LINUX  INTEL  Unclaimed  Idle    0,010 1775 0+00:10:34
slot20C117120067,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:30:46
slot10C132117164,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+06:36:22
slot20C132117164,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+00:20:06
slot10C146151146,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+03:35:04
slot20C146151146,i  LINUX  INTEL  Unclaimed  Idle    0,000 1775 0+06:33:10
slot10C172125196,i  LINUX  INTEL  Claimed  Busy    1,010 1775 0+06:28:20
slot20C172125196,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:28:23
slot10C181054058,i  LINUX  INTEL  Claimed  Busy    0,990 1775 0+06:29:13
slot20C181054058,i  LINUX  INTEL  Unclaimed  Idle    0,010 1775 0+00:18:51
C204151111.ipop    LINUX  INTEL  Owner    Idle    0,200 249  0+00:00:09

Total Owner Claimed Unclaimed Matched Preempting Backfill
INTEL/LINUX 32 1 19 12 0 0 0
Total 32 1 19 12 0 0 0

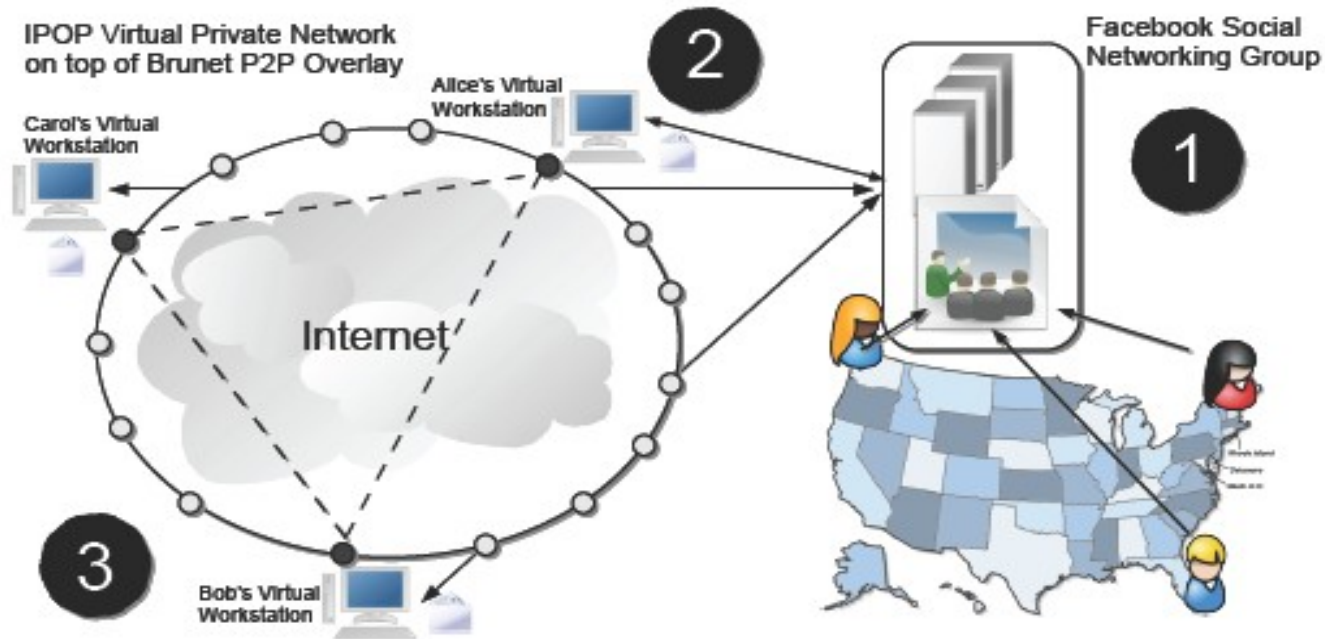
Favorite applications
debian 0 xmessage griduser@localh... 06:00:07 AM
```

IPOP Virtual Private Network

- Virtual LAN
 - **Self-configuring, decentralized virtual network**
 - P2P VPN routes IP packets over P2P overlay
 - IPsec provides security
- P2P Overlay
 - Structured P2P overlay
 - NAT/firewall traversal
 - **Robust, scalable, and self-organizing system**



3 Easy Steps



➤ Our Contribution

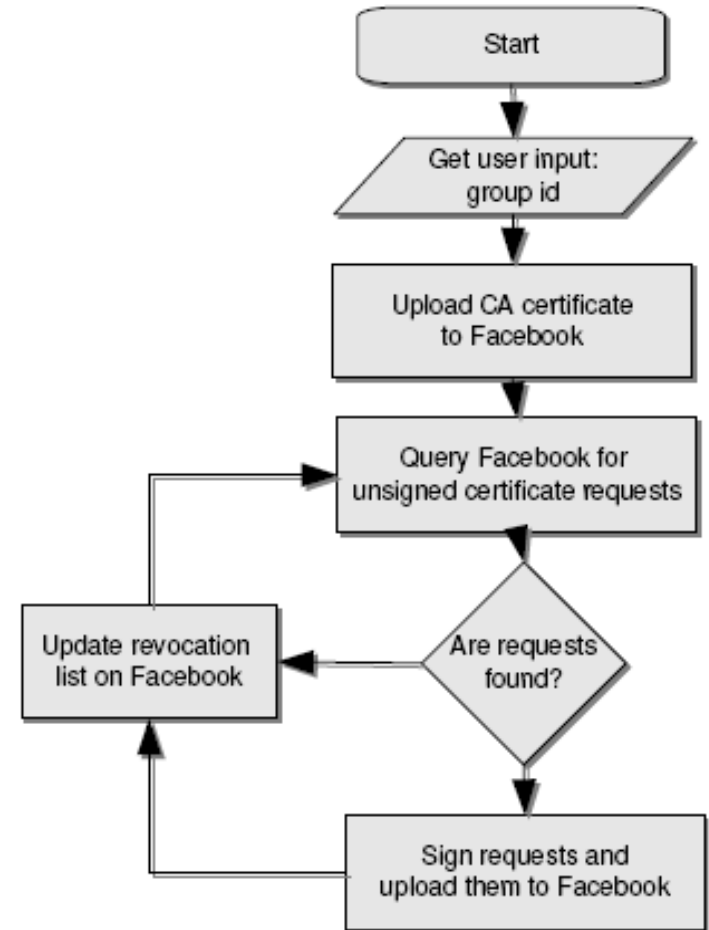
- **Hide the complexity of PKI/certificate management**
- Use social networking API to provide user with easy to use management

➤ The Process

- Users join social networking group
- Users run virtual machine and select group through Web interface
- Virtual machines form VPN

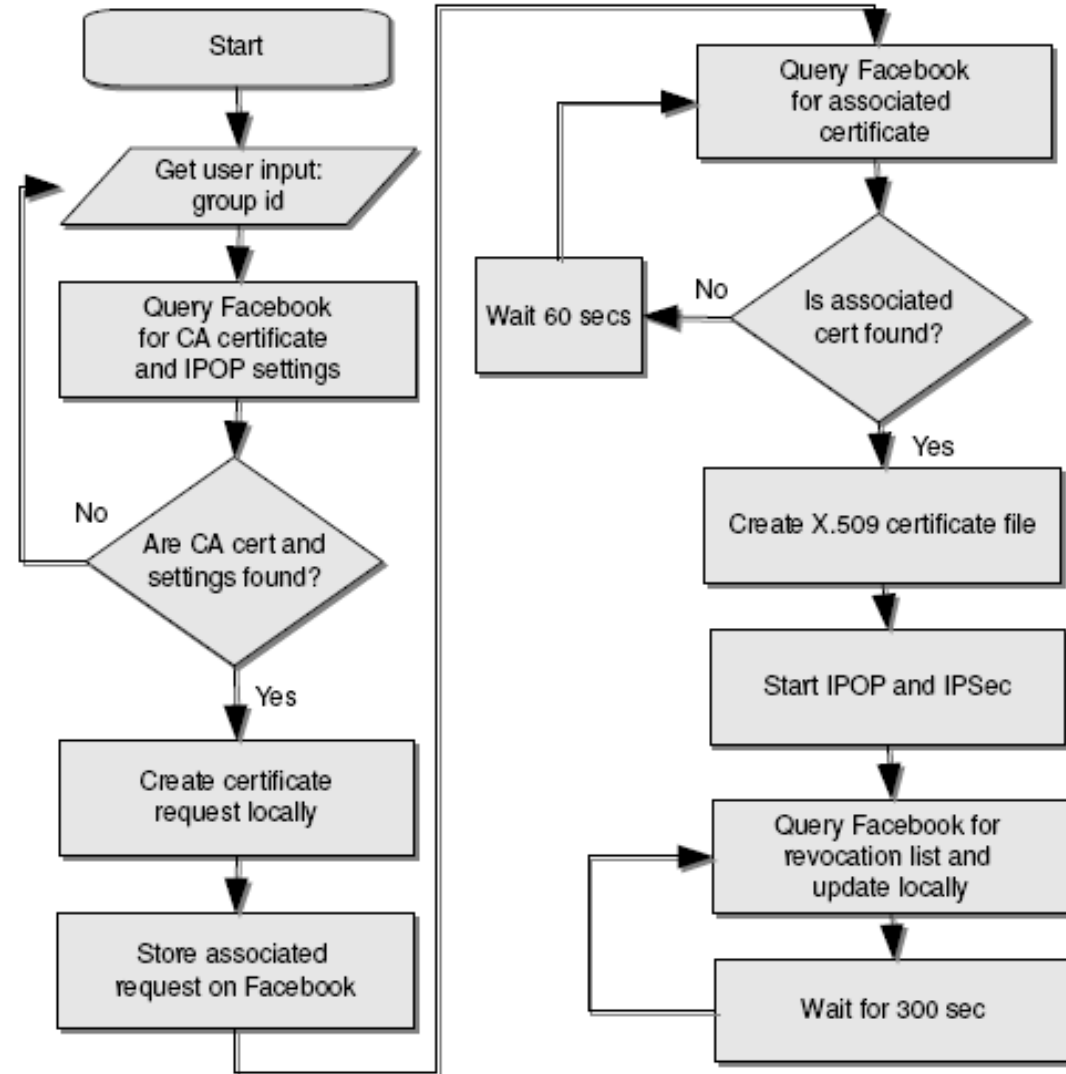
Certificate Management

- CA certificate management process
 - CA uploads its certificate to the group's datastore
 - Checks group's datastore for unsigned certificate requests
 - If requests found, sign the request
 - Store the signed certificates back on group datastore
 - Update revocation list, if necessary
 - Wait for a specific interval
 - Loop back to query step
- **This process is automated, the group creator only has to manage the social networking group**



Certificate Management (2)

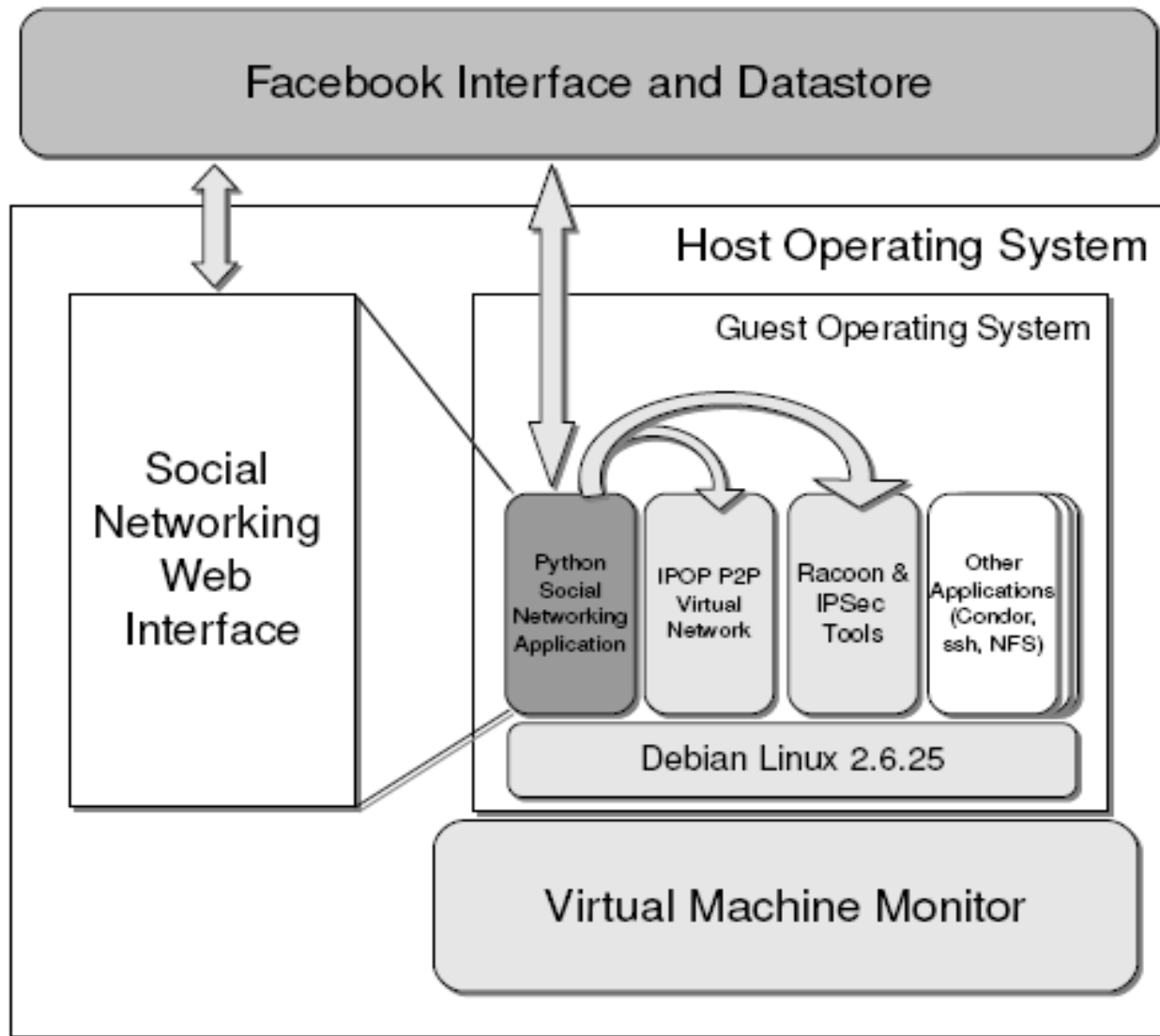
- Peer certificate acquisition
 - Query social networking group for CA certificate
 - Upload certificate request to group datastore
 - When signed certificate is available, configure and run VPN and IPsec
 - Retrieve revocation list from social networking datastore
- **Peer joins group and select group name through Web interface, social networking application handles the rest**



Implementation Details

- Grid Appliance
 - Debian Linux, kernel version 2.6.25
 - Condor job scheduler for cycle sharing
- Virtual Private Network
 - IPOP Router, open-source C# ,
 - Linux kernel tap device
 - IPSec and Racoon for security and IKE
 - OpenSSL tools for X.509 certificate management
- Social Networking Application
 - Written in Python 2.4
 - PyFacebook, Python libraries for Facebook API
 - Python-Django, web framework for user interface

Implementation Details (2)



Demo Video

**Time for a video,
we will continue slides after video**

Experiments and Analysis

- Ease of deployment
 - Peer joins Facebook group, downloads and runs virtual appliance
 - User navigates to <http://apps.facebook.com/securegridnet/> and selects group and node type
 - **Virtual workstation joins VPN in less than 5 minutes (one-time overhead)**
- Network Performance
 - We ran IPSec between two nodes in the same LAN to measure throughput
 - 2GB Ethernet network, 2.33 GHz dual core host with 8GB RAM, 256MB RAM per VM
- Performing Grid Tasks
 - **We successfully performed a BLAST job on a Condor pool of 4 virtual workstations**

Protocol	Without IPSec	With IPSec
TCP	51.5 Mbps	33.0 Mbps
UDP	45.4 Mbps	32.0 Mbps

Social Networking API Limitations

- Assumptions of Trust in Social Networks
 - Secure communication channel with social network
 - Data integrity and protection in social networking datastore
 - **Trust in social networking identity binding**
- Social network as a trusted medium
 - Trust retrieved CA certificate
 - Identify owner of certificate request
- Limitations of Facebook
 - Only HTTP access is provided through REST API, HTTPS is not yet available
 - **Integrity check is provided for HTTP POST, no encryption is available**
 - Facebook is still working on user permissions, access control is not yet available

Related Works

- Curry et. Al (2008)
 - HP lab project that used Facebook and virtual machines to provide employees access to legacy software
- Authenticatr (2008)
 - Use social links for authenticated out-of-band channel to enable secure communication channels by exchanging cryptographic keys through social networks
- Social Networking Standards
 - OpenSocial - open standards that defines API exposed to developers across different social networks
 - OpenID – distributed framework for digital identity consisting of multiple providers such as Yahoo.com, WordPress.com, LiveJournal.com
 - Oauth – open standard that describes how one system can grant limited access to another system on behalf of a particular user

Conclusion

- The bottom line
 - Social networking groups management can be mapped directly to certificate management
 - Access to a social networking group means acquisition of CA certificate and signed certificate
 - Removal from a group means invalidations of your certificates
 - **Access control to resources through social networking group management**
- Future Work
 - Integrate with OpenSocial-based social networks (MySpace, Orkut, LinkedIn)
 - Study other aspects of social networking in collaborative environments
 - **SocialVPN – self-configuring P2P VPN consisting of your social networking peers**

Thank you and Questions?

- We hope that this presentation provided some insights on the benefits of integrating social networking/Web 2.0 in grid computing environments.
- Contact Information
 - Pierre St Juste (me) – ptony82 at ufl dot edu
 - Dr. Renato Figueiredo (my advisor) - renato at acis dot ufl dot edu
 - David Wolinsky (my colleague) - davidiw at ufl dot edu
 - Jiangyan Xu (my colleague) - jiangyan at ufl dot edu
 - Dr. Michael Covington (Intel collaborator) - michael.j.covington at intel dot com
- **We welcome criticism, comments, and suggestions, feel free to contact us**