P2P Security Implementation-Groove

Haixia Yu

1. P2P Introduction

Peer-to-Peer (P2P) network can be simply defined as sharing of resources and services by direct exchange.

The Features of P2P are:
- Exchange information directly, rather than through intervening servers;
- Flexibility of system structure, a node can be a server of some nodes and at the same time it can also be a client of some other nodes.

In most P2P networks, even remote hosts can access the nodes in the P2P network. Programs and data are frequently transferred between systems in remote locations. So it becomes imperative for the P2P users to ensure their own security and the security of the local network.

2. Groove Security Service

2.1 Groove overview

Groove is a peer-to-peer software platform, which provides a virtual shared space concept. Peers who want to communicate among themselves will log on to a shared space and communicate among themselves. They have the right to include or reject any peer from that shared space. Programming can be done using VC, VB or JavaScript. To run this, the Groove platform must be running on all the peers. Groove is immediately useful for direct peer-to-peer multimedia communications related to projects, meetings, events, and relationships.

Fig1. Groove Architecture
2.2 Groove Security service

The essence of Groove is that two or more people can interact with complete personal control over the content, function and duration of a Groove ‘shared space.’ These spaces are rich in context and content, high in functionality, and convenient to create. Often, a user will invite members into a shared space across organizational boundaries on a spontaneous, ad hoc basis. Users interact in these shared spaces to solve a particular problem or address an opportunity, perhaps sharing sensitive information and conducting confidential business in the process.

a) Groove encrypts all content on disk and over the network.

Confidentiality, authentication, and integrity of the workgroup and its space are ensured at all times by strong security and encryption. Groove automatically encrypts all materials on the user’s disk and across the network as it travels between peers.

Groove uses strong, 192-bit encryption. Users create a passphrase to encrypt their account and shared spaces. A passphrase – a collection of words – provides for greater length and variety than a simple password, and makes it more difficult for someone with malicious intent to make an educated guess at a user’s secret code to enter into an existing account. In this way, even should a user lose his/her laptop or allow someone else access to his or her desktop, shared space content is protected. Even if an intruder gained access to the file system in which Groove spaces are listed, the contents of those spaces would remain encrypted and impossible to compromise without the user’s passphrase.

Furthermore, all content and activity within a shared space are sent across the network to all recipients. This traffic is also encrypted and can only be decrypted by other members of the shared space. Each change or addition to a Groove shared space is sent as a discrete “delta” or packet across the network to all other members of the space. Even in the unlikely event that an individual packet of information is intercepted; it could be decrypted only after massive decryption efforts. Even then, only that small amount of content would be compromised. The shared space and the rest of its contents would be safe from unauthorized access.

b) Groove authenticates users automatically and without any third-party intervention.

The purpose of Groove is to foster meaningful interaction among members of a shared space. To do so, the creation of a space must be a simple, intuitive and effortless task, not unlike the creation of a new email message or the making of a telephone call. In those instances, no one “asks permission” to neither make contact with external parties, nor do they seek the help of IT or others to set up the contact. In Groove’s peer-to-peer architecture, because there is no server-based administration of security, all security function and management is relegated directly to the peer devices themselves. However, if this approach imposes administrative complexity on the end user, it is likely that many people will either refuse to use this type of solution
at all, or do so in an a way that compromises security for the sake of simplicity. In other words, the peer computing environment must not only provide robust security, but must do so in a way that is effectively transparent to the user.

Groove users establish trusted relationships via the exchange of contact information in the form of vCards. A vCard is an electronic business card file (.vcg) based on a published industry specification. vCards, part of the Groove application functionality, include a person’s public key. There are a number of convenient ways that this exchange can occur between two or more people. Users can utilize these vCards [4] to ensure integrity and authentication throughout their communications.

In the likeliest inter-company, cross-firewall scenario, one member will send an email invitation to another. For example, say I email to you an invitation to a shared space. When you accept the invitation, you automatically have accepted my Groove vCard. Your reply (via Groove) sends to me your vCard in return. This peer distribution of keys ensures security without requiring centralized certificate and key management.

Furthermore, there are two additional methods available to users to more fully ensure that an invitation does indeed come from the person who sent it. This is important, since an invitation sent via email, for example, depends in part on how much the user trusts the email system itself.

- **Voice annotation.**
  Groove invitations include the ability to record a person’s voice. It’s an innovative approach to security that emulates the way that real people authenticate one another in real life. This approach uses human forms of recognition, as opposed to the typical methods used by public key infrastructure based systems in which you always trust that someone “notarizes” that you are who you say you are.

- **Digital fingerprints.**
  A user’s vCard includes that user’s public key. Groove uses that public key to compute locally on the recipient’s machine the sender’s digital fingerprint, a long, alphanumeric string of characters. The fingerprint is stored as part of the sender’s vCard. When a user receives a subsequent invitation, s/he can check the digital fingerprint in the invitation against the fingerprint in the stored vCard. If they match, the recipient can be assured that the sender is indeed who he claims to be.[4]

c) **Only invited members can participate in a Groove shared space.**
After you have accepted my invitation and we have authenticated each other, Groove then sends to you a set of keys and the shared space itself as well as a set of keys that allow you to decrypt the content of the space.
This exchange of keys for the space itself provides an easy mechanism for managing membership for the duration of a space. Throughout the normal lifecycle of a shared space, it is likely that new members will be invited and that other members will be “uninvited.” This presents a security challenge, since the “uninvited” member still retains the keys to the shared space. Whenever a member is uninvited from a shared space, Groove automatically issues a new shared space key to all members so that all subsequent data is protected and kept private from all past members. As far as the “uninvited” member is concerned, the “old” shared space is still on his or her local device(s), and he or she can still review the content and history of that space. However, he or she can no longer look at new content and activity.

d) Groove includes IT controls to safeguard against rogue components.

As a peer-computing platform, Groove provides users with extraordinary control over the functionality of a space itself. If any of the members decides that the shared space needs new or additional functionality, s/he can add new components or tools on the fly. When a user adds a tool, Groove sends a command to all the other users to do the same. If the other members already have the tool installed, Groove automatically adds the tool to the shared space. If any members do not have the tool installed yet, Groove (transparently to the user) locates and downloads the tool – from components.groove.net or any other recognized Groove component server. Groove installs the tool locally and adds it to the shared space.

Groove includes administrative controls that allow IT staff to “lock down” Groove desktops so that they may only download components that have been digitally signed (e.g., by Groove Networks or others) and/or that are found on approved server sites. This continues to allow end users a great degree of freedom while balancing necessary IT protections against viruses. [4]

2.3 Groove Security Implementation Summary

- All content and activity in a Groove shared space is confidential.
- Only authorized (authenticated) users have access to a shared space. Groove includes additional techniques to ensure authentication.
- Groove component management services guard against downloading of unauthorized tools.

3. References: