University of Macedonia
Master Information Systems
Networking Technologies
Professors:A.A Economides & A. Pomportsis

SECURITY IN PEER TO PEER NETWORKS

Patsiavoudi I. Eleftheria
M 22/05

Thessaloniki December 2005

Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Καθηγητές:Α.Α Οικονομίδης & Α. Πομπόρτσης

ΑΣΦΑΛΕΙΑ ΣΤΑ ΟΜΟΤΙΜΑ ΔΙΚΤΥΑ

Πατσιαβούδη Ι. Ελευθερία
Μ 22/05

Θεσσαλονίκη Δεκέμβριος 2005

TABLE OF CONTENTS

THE SPEED OF SECURITY, ARTICLE BY BRUCE SCHNEIER, IEEE SECURITY & PRIVACY, VOL.1, NO 4, JUL/AUG 03.REFER TO EVERY KIND OF ATTACK IN NETWORK. EXPLAINS HOW VULNERABLE PEER-TO-PEER NETWORKS MIGHT BE. GIVES INFORMATION ABOUT VULNERABILITIES SPREADS AND SOME ATTACK TOOLS, AND MAKES SOME SUGGESTIONS OF HOW YOU CAN KEEP YOUR NETWORK SECURE. 25

[12] HTTP://WWW.SPINELLIS.GR/PUBS/JRNL/2004-ACMCS-2P/HTML/AS04.HTML.....26

THIS REPORT SURVEYS PEER TO PEER CONTENT DISTRIBUTION TECHNOLOGIES, AIMING TO PROVIDE A COMPREHENSIVE ACCOUNT OF APPLICATIONS, FEATURES, AND IMPLEMENTATION TECHNOLOGIES. DEFINES THE BASIC CONCEPTS OF PEER TO PEER COMPUTING AND PRESENT THE MAIN ATTRIBUTES OF PEER TO PEER CONTENT DISTRIBUTION SYSTEMS AND THEIR ASPECTS OF THEIR ARCHITECTURAL DESIGN.....26

[13]COMPUTER SYSTEM AND NETWORK SECURITY, PAGE 144-146.....26

GREGORY B. WHITE, ERIC A. FISCH, UDO WR. POOCH.....26

CRC PRESS.....26

[14]SHANE BALFE, AMIT D. LAKHANI, KENNETH G.PATERSON.....26

TRUSTED COMPUTING: PROVIDING SECURITY FOR PEER TO PEER NETWORKS …26

PROCEEDINGS OF THE FIFTH IEEE INTERNATIONAL CONFERENCE ON PEER TO PEER COMPUTING (P2P'05).....26

2005 IEEE.....26

[15]HTTP://WWW.ECE.RUTGERS.EDU/~PARASHAR/CLASSES/01-02/ECE579/SLIDES/SECURITY.PDF.....26

[16] HTTP://WWW.WEBOPEDIA.COM/DIDYOUKNOW/INTERNET/2005/PEER_TO_PEER.ASP. 26

SUMMARY

This paper's theme is security in peer to peer networks. Firstly, it is shown p2p architecture and its major types of network. Secondly, it is presented some security threats in today's p2p networks. Moreover, applications -aimed to security and persistence- are listed and valued. In chapter 4, we try to describe some elements of secure systems and analyze how authentication, authorization, and encryption are established, whereas in chapter 5 major security technologies are valued. Furthermore, we describe how to build a secure p2p network in an enterprise environment. Security advantages and disadvantages are described also. In chapter 9 we conclude with a proposal for future researches.

Το θέμα της εργασίας είναι η ασφάλεια στα ομότιμα δίκτυα. Αρχικά, παρουσιάζεται η αρχιτεκτονική τους καθώς και οι κύριες μορφές των ομότιμων δικτύων. Στη συνέχεια, αναφέρονται οι κίνδυνοι που εμφανίζονται στα δίκτυα αυτά. Έπειτα, γίνεται μια προσπάθεια αξιολόγησης των εφαρμογών ασφάλειας και διατήρησης. Στο 4 κεφάλαιο, περιγράφονται τα θεμελιώδη στοιχεία ενός ασφαλούς συστήματος και πως αυτά καθιερώνονται, ενώ στο 5 αξιολογούνται οι κύριες τεχνολογίες ασφάλειας. Συνεχίζοντας, περιγράφουμε την ανάπτυξη ενός ασφαλούς ομότιμου δικτύου σε επιχειρησιακό περιβάλλον. Ακόμη, περιγράφονται τα αρνητικά και θετικά στοιχεία των p2p. Στο 9 κεφάλαιο ολοκληρώνουμε με τα συμπεράσματα μας και με μια πρόταση για μελλοντική έρευνα.

1 Peer-to-peer Architecture

Often referred to simply as peer-to-peer, or abbreviated P2P, peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures where some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler but they usually do not offer the same performance under heavy loads. The P2P network itself relies on computing power at the ends of a connection rather than from within the network itself.

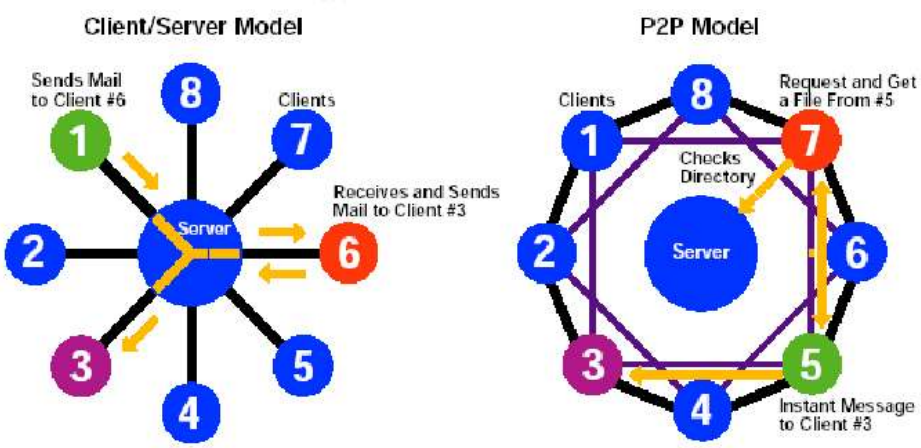
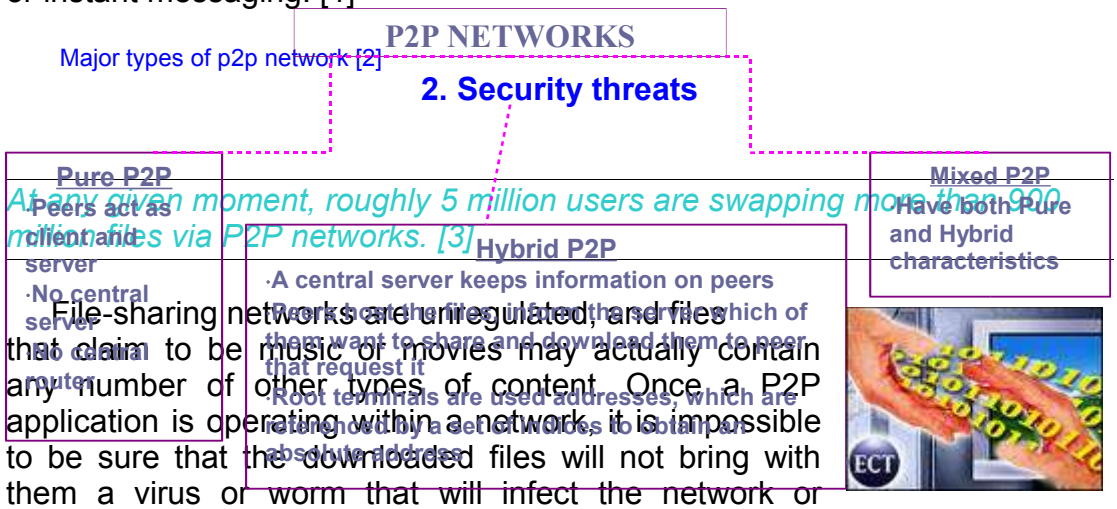


Figure 1 illustrates the difference between the client/server and the P2P models

P2P is often mistakenly used as a term to describe one user linking with another user to transfer information and files through the use of a common P2P client to download MP3s, videos, images, games and other software. This, however, is only one type of P2P networking. Generally, P2P networks are used for sharing files, but a P2P network can also mean Grid Computing or instant messaging. [1]



File-sharing networks are unregulated, and files that claim to be music or movies may actually contain any number of other types of content. Once a P2P application is operating within a network, it is impossible to be sure that the downloaded files will not bring with them a virus or worm that will infect the network or

spyware that is designed to track users' actions, and possibly collect confidential information.

2.1 Spyware and adware

Spyware is any technology used to gather information about computer users or their activities, secretly or without consent, and relay that information to interested and potentially undesirable third parties over the Internet. Adware also sends information to third parties, though with the user's often uninformed permission. Examples of spyware and adware include keylogging, Web bugs, and tracking cookies.

More people looked for information about the file-swapping program Kazaa than any other topic on the Net in 2003, according to search site Yahoo.

For example, when a user downloads and installs the free Kazaa software, additional software from third-party providers, such as Cydoor, Topsearch, and GAIN AdServer, is also downloaded.[4]

Kazaa's terms of service agreement points out that Cydoor, a maker of adware software, may use the "Internet connection to update its selection of available ads and store them on [the user's] hard drive." But this information may be buried within thousands of words, and most people blindly click the "Agree" button without reading all the fine print.

Since adware/spyware is a piggyback program that runs separately from the program it accompanies, it uses additional processing power, hard drive space, and bandwidth, and may have security flaws itself, opening an avenue of attack for hackers or viruses [5]. When it is downloaded surreptitiously, as in the case of the Kazaa download, it can bypass corporate firewalls and enter the network, rendering sophisticated perimeter security technology ineffective.

2.2 Exposure to viruses and worms

The Slammer worm was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes." For the six months prior to the Sapphire (or SQL Slammer) worm's release, the particular vulnerability that Slammer exploited was one of literally hundreds already known.[6]

P2P networks can be, and are, easily exploited to distribute viruses and worms, allowing them to bypass normal security and filtering barriers. Viruses and worms can hitch a ride on files transferred using P2P applications and make their way into corporate networks.

Most famous P2P worms: Kitro, Lolol, Benjamin, Roron.

P2P applications allow users to send files directly to each other, effectively circumventing perimeter security mechanisms, and enabling viruses to easily penetrate and then propagate within a network. [7]

45 percent of the most popular files shared on Kazaa—including “cracks” that let users break copy protection on commercial software—actually contain viruses, worms, or Trojan horses. [8]

2.3 P2P vulnerable to hackers

Hackers can easily take advantage of P2P vulnerabilities, including buffer overflow, to spread worms and viruses. A buffer overflow is a software glitch that causes problems for users and software developers. In May 2003, version 2.02 of Kazaa software was reported to have buffer overflow vulnerability. Computers running Kazaa and acting as Supernodes are vulnerable to attacks if they receive packets with more than 200 IP addresses of other Supernodes. “A remote user can send 203 entries to the target Supernode to trigger the flaw and cause the Supernode to crash” or execute code on the victim’s computer. Vulnerabilities in P2P networks also occur during the process of transferring files. When a user transfers files, his or her IP address is revealed. Using this IP address, hackers can potentially attack the system. Most P2P software can be manipulated to create and slip through holes in the security architecture of a network. [9]

2.4 Loss of confidential information

Users can accidentally or intentionally make confidential information available to P2P users around the world in one of two ways. They can place confidential files (which should be properly safeguarded) in a shared folder. Or they can configure the P2P file-sharing application incorrectly so that their entire hard disk, computer, or even network drives are set up as available to share. When this happens, anyone on the P2Pnetwork may be just moments away from downloading personnel files, financial results, or a customer database. [10]

2.5Denial of Service

Every user of a p2p program is soaking up the network bandwidth. Software like Napster, Gnutella and Scour are generally used to download relatively large files as MP'3s, AVIs, MPGs, JPGs. If enough users are downloading these files types of files, this can cause network resources to be tied up, resulting in a denial of service (DoS) [11].In addition to network bandwidth, full hard disks can also result in a denial of services .If you can't save the file that you are working on, you will stop working to avoid the risk of losing the work.

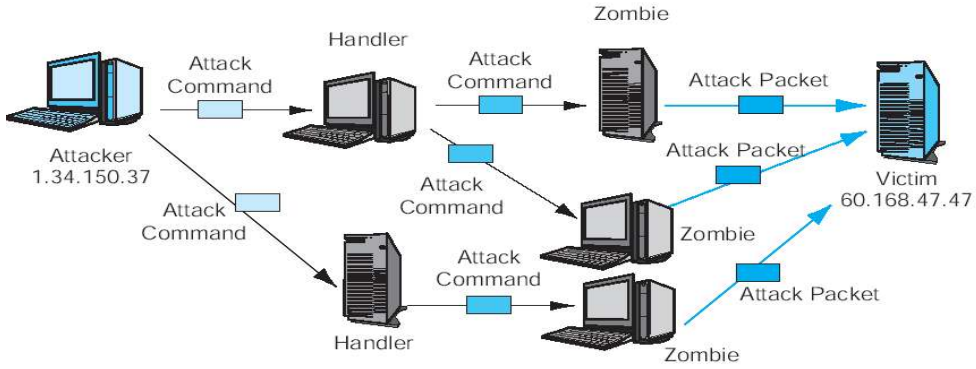


Figure 2: disrributed Flooding Denial of Service Attack

Had at Least One Security Incident in this Category (May have had several)	Percent Reporting an Incident in 1997	Percent Reporting an Incident in 2003	Number Reporting Quantified Losses in 2002	Average Reported Annual Loss per Firm (Thousands) in 1997	Average Reported Annual Loss per Firm (Thousands) in 2002
Viruses	82%	82%	254	$76	$200
Insider Abuse Of Net Access	Not Asked	80%	180	Not Asked	$136
Unauthorized Access by Insiders	40%	45%	72	NA	$31
Denial of Service	24%	42%	111	$77	$1427
System Penetration	20%	36%	88	$132	$56

Figure 3: CSI/FBI Survey Copyright 2004 Prentice-Hall. Survey conducted by the Computer Security Institute (www.gocsi.com).Based on replies from 530 U.S. Computer Security Professionals. [12]

3. Peer-to-peer Applications

3.1 Peer-to-Peer "File Exchange" Systems

These systems are targeted towards simple, one-off file exchanges between peers. They are used for setting up a network of peers and providing facilities for searching and transferring files between them. These are typically light-weight applications that adopt a best effort approach without addressing security, availability and persistence.

System	Brief Description
Napster	Distributed file sharing-hybrid decentralized
Kazza	Distributed file sharing–mixed decentralized
Gnutella	Distributed file sharing–purely decentralized

3.2 Peer-to-Peer Content Publishing and Storage Systems

These systems are targeted towards creating a distributed storage medium in-and through-which users will be able to publish, store and distribute content in a secure and persistent manner. Such content is meant to be accessible in a controlled manner by peers with appropriate privileges. The main focus of such systems is security and persistence, and often the aim is to incorporate provisions for accountability, anonymity and censorship resistance, as well as persistent content management (updating, removing, version control) facilities.

Table 1: Classification of current peer-to-peer systems RM: Resource Management; CR: Censorship Resistance; PS: Performance and Scalability; SPE: Security, Privacy and Encryption; A: Anonymity; RA: Reputation and Accountability; RT: Resource Trading. [13]

System	Brief Description	Main Focus
Scan	A dynamic, scalable, efficient content distribution network. Provides dynamic content replication	PS
Publius	A censorship-resistant system for publishing content. Static list of servers. Enhanced content management (update and delete).	RM
Groove	Internet communications software for direct real-time peer-to-peer interaction.	RM,PS SPE
FreeHaven	A flexible system for anonymous storage	A,RA
Freenet	Distributed anonymous information storage and retrieval system.	A,RA
MojoNation	Distributed file storage. Fairness through the use of currency mojo.	SPE RT
Oceanstore	Architecture for global scale persistent storage. Scalable, provides security and access control.	RM,PS SPE
Intermemory	System of networked computers. Donate storage in exchange for the right to publish data.	RT
Mnemosyne	Peer-to-peer steganographic storage system. Provides privacy and plausible deniability	SPE
PAST	Large scale persistent peer-to-peer storage utility	SPE
Dagster	A censorship-resistant document publishing system.	CR,SPE
Tangler	A content publishing system based on document entanglements.	CR SPE

4 The elements of secure systems

While the P2P domain might seem exciting and new, the elements of secure computing in a distributed environment remain the same. Trust is established by a combination of these standard elements:

- **Authentication.** The process of determining whether or not some entity is in fact who or what that entity declares itself to be. In practical terms, authentication comes in two forms. The first form involves peers authenticating themselves to other peers over a network such as the Internet. The second form involves users of a P2P application authenticating themselves to the application. In some P2P applications, these two forms are the same.
- **Authorization.** The process of giving an authenticated entity permission to do some action or access some resource. In a P2P application, a peer might be authenticated to access some subset of the resources on another peer.
- **Encryption.** The process of converting readily understandable information (plaintext) into a form difficult to understand by unauthorized individuals and systems (ciphertext). Decryption is the reverse of this process.
- **Access Control.** Protects against unauthorized use of the network or its resources.
- **Confidentiality.** Ensures that an unauthorized individual does not gain access to data contained on a resource of the network.
- **Integrity**. Ensures that data is no altered by unauthorized creation of data
- **Usage**. Ensures the resources of the network are reserved for use only by authorized users in an appropriate manner.[14]

Additional services not explicitly included in could be added to the list, such as accountability and anonymity .Any particular network may require a combination of all, some or none of these various security services. [15]

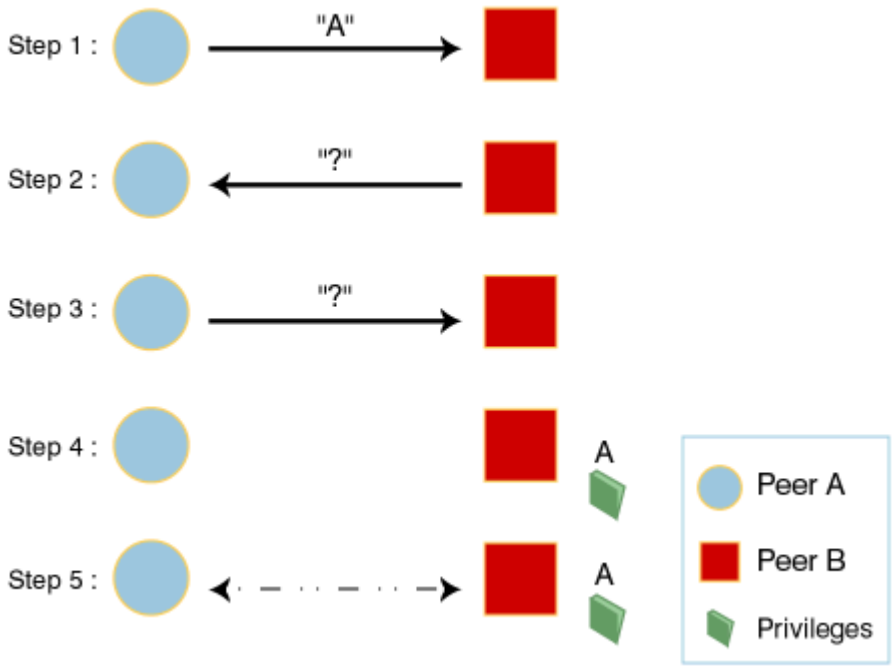
In a P2P application, encryption can play many roles. One obvious use of encryption is to protect the information that flows between peers on an unsecured network such as the Internet. This, combined with secure authentication of each peer, ensures that the exchanged data won't be eavesdropped upon during communication. If the information is digitally signed or a MAC (Message Authentication Code) is added to the information, both parties can be sure that the information wasn't modified, as well. [16]

As you will see in the examples below some of these elements are combined to create a secure distributed application.

4.1 Security in practice

To better understand how authentication, authorization, and encryption help establish trust between peers in a P2P application, let's consider the example shown in Figure 1.

Figure 3: Sequence of operations between peer A and peer B



Peer A on the left desires to initiate secure communication with peer B on the right.

i. Peer A connects to peer B and announces its identity.

ii. Peer B asks peer A to *authenticate* itself. Authentication can occur in many ways. Both peer A and peer B can use a shared key to exchange a secret message, or peer A can use the private key that corresponds to a public key that peer B holds to perform the same operation.

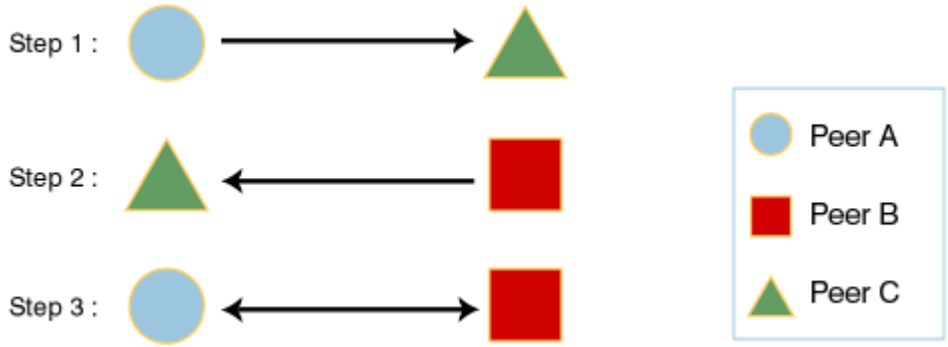
iii. Peer A asks peer B to authenticate itself.

iv. Peer B *authorizes* peer A to access certain resources by assigning privileges to peer A.

v. Before further communication takes place, the two peers can arrange to *encrypt* the channel connection between them.

If peers A and B haven't met, they must rely on a trusted third party, peer C, to arrange an introduction, as shown in Figure 4.

Figure 4. Peer C introduces peer A and peer B



Here is the sequence of operations for the introduction:

i. Peer A initiates secure communication with peer C as described above. Peer C gives peer A the information necessary to authenticate peer B. This may include peer B's public key, a shared key, or a token or certificate that enables the communication.

ii. Peer B initiates secure communication with peer C and performs the same operations.

iii. Once this information has been transferred, peer A may initiate communication with peer B.

The method described above follows the pattern used by standards such as SSL[2] .

4.2 How safe is the content?

If you trust an entity you might be tempted to trust the content it provides. In some cases, this assumption is reasonable. If the content being accessed contains information about the entity being the origin of the information, or if it contains the information from a service that the entity provides, the fact that you trust the entity is enough justification to trust the content you get from the entity.

If, on the other hand, the entity is not the origin of the content, but is acting as a cache or intermediary for the content, it might be wise to validate the content. Certain kinds of content, such as active content (applets), are dangerous enough that validation should be mandatory.

There are many ways to validate content, including simple checksums, encryption and watermarking. Above, it is described a mechanism based on digital signatures.

[2] SSL Secure Sockets Layer protocol offers asymmetric authentication and private communication, SSL assures that the one peer has a particular identity and enables the peers to agree on a private key which can be used in subsequent communication

i. Peer A establishes a secure connection with peer B as illustrated in Figure 3.

ii. After it establishes the channel, peer A requests a piece of content from peer B. If peer B originates the content, it digitally signs the content before transferring it. If peer B is merely distributing content created elsewhere, the content is already signed.

iii. After peer A receives the content, it verifies the digital signature attached to the content.

The verification of many types of content is already standard operating procedure for many mainstream applications. It must become standard operating procedure for P2P applications as well. [17]

5 Network Security Technologies

There are many network security technologies –identity technologies, network firewalls, content filtering, cryptography –.Yet, since P2P file sharing systems are rapidly becoming one of the most popular applications on the internet, with millions of user online exchanging files daily. [18] It is important to describe host and application security technologies, identity technologies

Host and application security relates to the technologies running on the end system to protect the operating system, file system, and applications.
Identity technologies are concerned with verifying who the user is on a p2p network

The following describes the 10 table rows and the rating scale for each:

- **Difficulty in attacker bypass** – (1=seriously consider if it is worth deploying this technology; 5=best of luck, script kiddie!).
- **Ease of network implementation** –refers to how hard the technology is to integrate into the network; (1=better staff up; 5=no worries).
- **User impact**-Refer to the impact, if any, the technology has on the users. For example whether users complain about application failures, experiences effects on their day-to-day factions (1=are you sure you want to deploy this; 5=users won't notice).
- **Application transparency**-Refers to whether any significant changes are necessary to corporate applications or to the security technology in support of those applications to make effective use of this technology (1=check your brakes before you get the road; 5=minimal changes necessary).
- **Maturity of technology**-(1=flash-in-the-pan-technology;5=such technology as one-time passwords).
- **Ease of management**-How the product is managed and the operational costs of deploying and managing the technology (1=dedicate staff often required [high costs]; 5=almost no management is required [low cost]).

- **Performance-** compares the performance of the network with and without the security technology (1=significant impact;5=no one will notice).
- **Scalability-**Whether the technology becomes significantly harder to deploy, manage as the network grows (1=very difficult to scale;5-size of network has almost no impact).
- **Finance affordability**-This number assumes a midsize network and that the technology is deployed in the most relevant areas. Also, this rating is based on the price of the product. (1=too expensive for most networks; 5=almost free of charge).

Name	File system integrity checking	Host-based (personal) firewalls	Host Intrusion Detection Systems-HIDS	Host Antivirus
Common example	Tripwire	IPFilter	Entercept	McAfee VirusScan
Attack elements detected	·Application manipulation ·Rootkit ·Virus/worm/Trojan	Probe / scan	·Probe/scan ·Direct access ·Application manipulation ·TCP SYN flood ·Transform redirection ·Remote control software	
Attack elements prevented		·Direct access ·Remote control software	Real following description	·Virus /Worm /Trojan horse ·Remote control software
Difficulty in attacker bypass	4	2	4	3
Ease of network implementation	5	2	5	5
User impact	4	2	4	3
Application transparency	5	1	2	4
Maturity of technology	5	2	2	5
Ease of management	3	1	2	4
Performance	5	4	4	4
Scalability	3	2	3	4
Financial affordability	5	3	3	4
Overall value of technology	61	51	61	66

Table 2 shows summary information for the host application security

As you expect host AV scores the best out of the brunch. File system checking and HIDS also score well. You can't go wrong with any of these technologies. Plenty of organizations use all of them in different parts of their

networks: host AV almost everywhere, file system checking on all peers, HIDS on some key peers.

Table 3 shows summary information for the identity technologies

Name	**Reusable passwords**	**OTP (One time password)**[3]	**PKI**[4]	**S C**	**s**
Common example	UNIX username/ password	RSA SecurID	Entrust Authority PKI	Gemplus	New market
Attack elements detected	Identity spoofing				
Attack elements prevented	Direct Access	Identity Spoofing Direct Access	Identity Spoofing Direct Access	Identity Spoofing Direct Access	Identity Spoofing Direct Access
Difficulty in attacker bypass	2	5	3	4	3
Ease of network implementation	5	4	2	2	1
User impact	4	2	2	2	4
Application transparency	5	3	3	2	1
Maturity of technology	5	5	3	2	1
Ease of management	4	2	1	2	3
Performance	5	4	4	4	3
Scalability	3	4	3	4	3
Financial affordability	5	3	3	2	1
Overall value of technology	59	63	54	55	52

[3] Most OPT operate on the principle of two-factor authentication.
[4] PKI is designed as a mechanism to distribute digital certificates that verify the identity of the user

Security systems of the near future will validate IDs using the unique individual patterns of nose hair growth.

From this chart, based on weightings and rankings, OTP seems to provide the most overall security while encountering the least amount of detrimental ratings among the technologies. Although all of PKI variants scored lower, their use in specific applications is unavoidable. IPsec gateways in site-to-site VPN, for example can't take advantage of OTP because there is no one there to enter the passcode when they authenticate with another peer [19].

6 Secure p2p in an enterprise environment

Today's enterprises are enjoying the benefits of greater communication with fewer boundaries between them and their business partners, customer and employees. Yet, they are more likely than ever to be victims of worms, viruses, denial of service attacks, and on-line fraud or theft.

Merely one virus, the My Doom e-mail virus, is estimated to cost companies €22.6B (mig2 intelligent Unit)

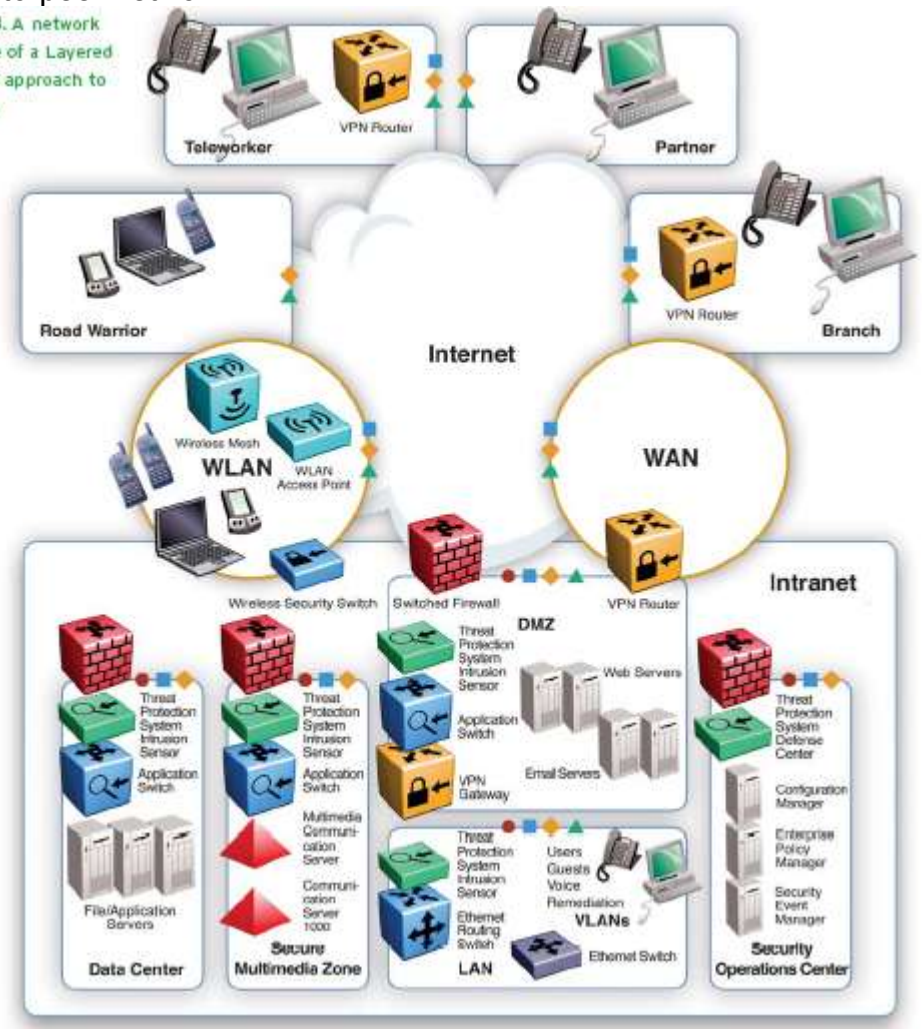
A properly designed and implemented security policy is an absolute requirement for all types of enterprises and should be a living document and process, which is updated to reflect the latest changes in the companies' infrastructure and service requirements. It is important to use multiple approaches to security enforcement at multiple areas with in a network, so as to protect the entire enterprise network-remote and local network user, data and multimedia, wired and wireless connections.

- **30 to 40%** of Internet use in the workplace is not related to business (IDC Research).

- **37%** of workers say they surf the Web constantly at work (Vault.com)

Here is an example of how to build a secure enterprise environment using peer-to-peer network

Figure 3. A network example of a Layered Defense approach to security



♦perimeter security •Core network security □secure communications ▲endpoint security

- **Endpoint security-**ensures valid identity and connected device security policy compliance
    1. **Internal endpoint security**: protection of internal devices. . Use of Ethernet switch and Ethernet routing switch to verify if someone connecting to inside the network is in fact a legitimate user.
    2. **Wireless local Area Network(WLAN)-**specific protections to ensure security for the wireless network segments (WPA[5]→wireless user authorization and TKIP[6]→layer encryption mechanisms)
    3. **Remote endpoint security**

[5] WPA: WiFi protected access (security standard)
[6] TKIP: Temporal Key Integrity Protocol

- **Perimeter security**-keeps the “good stuff ” in and the bad stuff out by securing the boundaries between zones of different level of trust . Use of firewalls

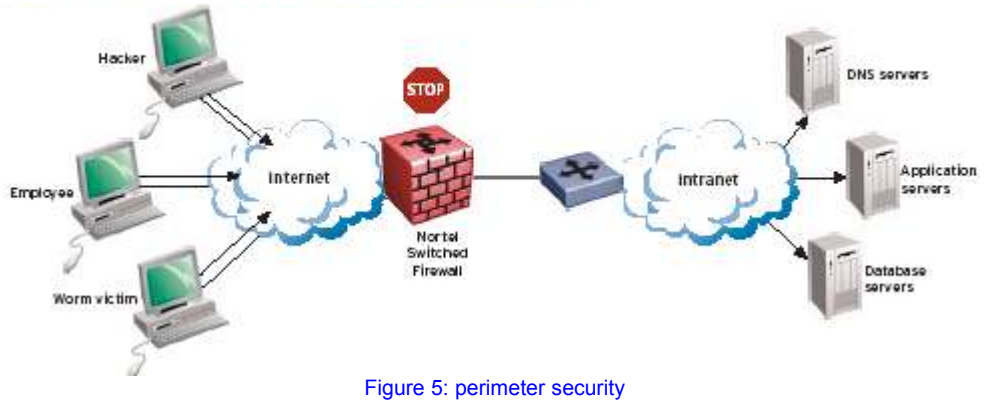


Figure 5: perimeter security

- **Secure Communications** – ensures information protection from unauthorized discovery over the network
- **Core Network Security**-keeps watch for malicious software and traffic anomalies, network policy and enabling survivability[20]

Above is described an architecture of a secure p2p network Based on open standards-based solutions, this approach enables easy integration and simplified operations that reduce the overall network security total cost of ownership.

6.1The Future OF P2P Business Use

The future of any technology is murky at best, especially in a sluggish economy, and P2P still has some issues to resolve. Whether or not businesses decide to jump on the P2P bandwagon, the current lack of security features in P2P applications must be remedied. User authentication, file permissions, and file integrity are just a few of the security issues that need resolving-most likely through the use of client certificates and strong encryption. The addition of P2P proxy servers would provide additional control over internal users' access to a P2P network by limiting mainly bandwidth and content.

The next step is for businesses to realize that the potential of distributed processing and distributed file systems is too promising to ignore. Rather than spend money on expensive server class hardware, businesses could instead rely upon a distributed network of workstations. These workstations would

each maintain a small chunk of the corporate data locally, as well as offer spare processing cycles to applications that need it. The ultimate P2P business system would be completely distributed, applications included. Backups would be greatly simplified, as the data would be redundant by default (i.e., the same piece of data would sit on multiple computers); such a system adds resiliency as well. Also, hardware failures could be handled easily since each system would be identical and thus cheaper to replace or repair. [21]

7 Advantages and disadvantages of peer to peer networks

7.1 A few security advantages

- **Privacy**

Since a message can be sent between two peers without going through a centralized server, there's no way an intruder on the server can read the message

- **No central point of knowledge**

Since content can be replicated un-deterministically anywhere on a P2P network, it is impossible for an intruder to know the location of all copies. As a result content corruption and denial-of-services attacks can't be performed that easily.

- **Web of trust**

When interacting with each other, peers can establish their own level of trust. In a P2P environment, this can be achieved by the trust established between the domains.P2P systems then can refine the general trust level to suit their interactions.

- **Locality**

When searching, a peer will ask another peer in its local domain first. As a result, bad behaviour is limited to neighbours or direct contacts. When a server is contaminated, so are all its clients [22]

7.2 And some others …..

- All client provide resources –bandwidth, storage space, computing power).Thus as peers arrive and demand on the system increases, the total capacity of the system increases.

- The distributed nature of p2p networks increases robustness in case of failures by replicating data over multiple peers, and in pure P2P systems by enabling peers to find the data without relying on a centralized index server.
- The empowerment of the peers in association with a central index, makes the system fast and efficient to locate available content.
- Ease to use-simpler network than client/server
- There is a world of free stuff just waiting to be download[23]

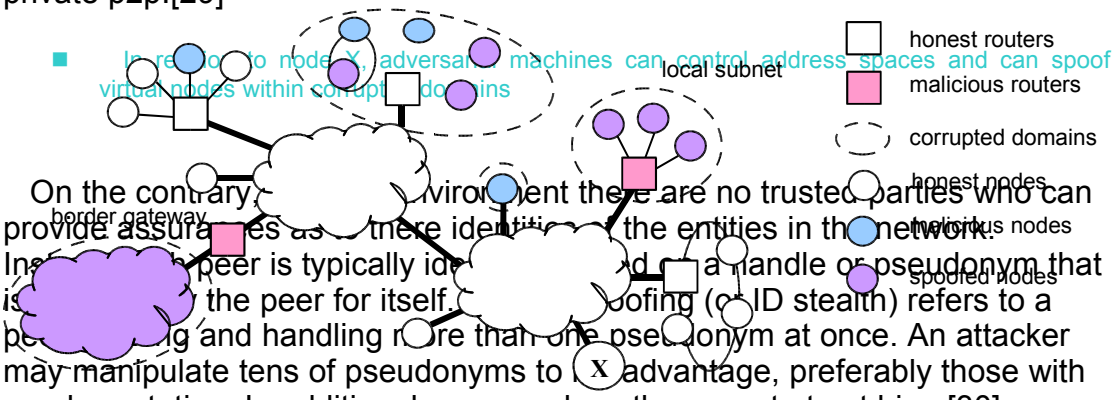
7.3 Attacks on Peer-to-peer networks

Many peer-to-peer networks are under constant attack by people with a variety of motives.
Examples include:

- poisoning attacks (providing files whose contents are different than the description)
- denial of service attacks (attacks that may make the network run very slowly or break completely)
- defection attacks (users or software that make use of the network without contributing resources to it)
- insertion of viruses to carried data (e.g., downloaded or carried files may be infected with viruses or other malware)
- malware in the peer-to-peer network software itself (e.g., the software may contain spyware) [24]
- filtering (network operators may attempt to prevent peer-to-peer network data from being carried)
- identity attacks (e.g., tracking down the users of the network and harassing or legally attacking them)
- spamming (e.g., sending unsolicited information across the network-not necessarily as a denial of service attack) [25]

8. Whom do you trust?

Trust id an every non-trivial peer-to–peer applications. In a distributed application, the level of trust is the metric that measures how confident we are that we are communicating with whom we think we are, and that we are accessing the recourses we think we are. [26]Reputation on the other hand is a peer's belief in another peer's capabilities received from other peers. [27] Although trust and reputation developed are different in how they are developed, they are closely related. Both of them are important so as to find a good peer which provides quality services.[28]When a peer finds "trustful" peers, a new type of network is created , called F2F (friend to friend) or private p2p.[29]



On the contrary, in the environment there are no trusted parties who can provide assurances as to the identities of the entities in the network. In addition, each peer is typically identified by a handle or pseudonym that is chosen by the peer for itself. Sybil spoofing (or ID stealth) refers to a peer creating and handling more than one pseudonym at once. An attacker may manipulate tens of pseudonyms to its advantage, preferably those with good reputation. In addition, he persuades other peer to trust him. [30]

In addition, it is vital to establish peer authentication and authorization (see page 9) and used them as protection from malicious peers. Also it is useful to understand the importance of trust management[7][8] and trust measures, so as users can rate the reliability of parties they deal with and share this information to their peers. This will help create trust among good peers as well as identify the malicious ones.

Conclusion

P2P architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. This kind of systems became immensely popular in the past few years, especially because of they offered way for people to get music, movies etc without payment.

Just as there are security issues with other computing models p2p adds it's own take on security issues specifically maleware, vulnerability to hackers, denial of access. These threats are malicious for the network and

[7]

[8] management of access control identity and general security issues (confidentiality, data integrity, non repudiation) in a network

considerable disadvantages, yet they cannot stop the growing popularity of peer to peer networks.

As far as applications are concerned, p2p are subdivided in two main groups, the file exchange system and the content publishing and storage systems. One of the basic aim of the last category is security .A classification of this group is provided accompanied with a note for there main focus.

The first step of securing your p2p system is to adopt a strict usage policy within workplace. To secure your network against the malicious threads described above there are many technologies to use. We describe the identity technologies as well as the host-application technologies and compare them.

As a conclusion, we propose that a good antivirus and the use of OTP (one time password) technology are a good way of solving your security problem.

Peer to peer networks are not only popular with home users but many business have come to rely on this cost-effective solution for sharing files with co-workers and client. Even the best protected organizations find it difficult to effectively shield themselves against all malicious security attacks due to the increasing rate with which they appear and spread. In this section we describe in summary a way to build a secure peer to peer network. A combination of developing and enforcement security policies that address the technical, business and human aspects of security choosing the right security solutions and putting the appropriate processes in place will help enterprises there challenges directly.

Peer to peer networks have both advantages and disadvantages. A list of pros and cons of p2p is listed above. The attacks are serious, yet using the technology described you can build a secure and quality network.

It is very difficult to find a trusted peer so it is important to establish authentication and authorization. We provide some concerns about the third trusted parties in p2p networks, so as to give adequate information about the “wired” peers and their content.

In the end, we propose a platform based in p2p technologies in which the computers participating as peers of a network automatically notify each other of security threats they receive. Based on the rate of warning messages received, the system will increase or decrease the security measures taken by the vulnerable applications running on the computer.

REFERENCES

[1] http://www.sans.org/rr/whitepapers/threats/468.php
Article written by Chris McKean (August 2001), refers to Intel's Peer-to-Peer Trusted Library. Explains the p2p network architecture and compares it with the client/server's one. Underlies the p2p security concerns and explains how the Intel's Trusted Library overcomed with them and allows the software developers to add the elements of trust to their p2p applications.

[2] http://en.wikipedia.org/wiki/Peer_to_peer_network
Summarizes some characteristics of peer to peer networks. Starts with their operations and their advantages- disadvantages.Explanes how academic p2p work and puts p2p under US law. Gives a detailed list of p2p applications and network protocols in alphabetical order.Ends with some multi-network applications/protocols/operating systems.

[3]International federation Industry [IFI] 2002

[4] http://enterprisesecurity.symantec.com/PDF/malicious_threats.pdf
Discusses the malicious threats of peer to peer networks. Explains how the usage of peer to a peer to peer network creates a hole in a firewall and can lead to the exporting of private and confidential information. Therefore administrators should begin analyzing their networks for p2p network usage and configure firewalls and systems accordingly to limit or prevent their usage.

[5]Computer Networks
E. Spafforg D. Zamboni
Page 548

[6]http://research.microsoft.com/projects/SWSecInstitute/slides/Wallach.pdf
The Speed of Security, article by Bruce Schneier, IEEE Security & Privacy, Vol.1, No 4, Jul/Aug 03.Refer to every kind of attack in network. Explains how vulnerable peer-to-peer networks might be. Gives information about vulnerabilities spreads and some attack tools, and makes some suggestions of how you can keep your network secure.

[7] Dr. Dobbs's Journal, page 41
June, 2004

[8] Trusecure, December 2003, page 33

[9]http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci929175,00.html
Refers to the vulnerabilities of peer to peer applications and to the entry points of the peer to peer networks. Analyzes the ICQ messaging program and the risks it may be generates. Gives useful advice to help you secure your peer to peer network. Ends with some advantages and disadvantages of the
peer to peer applications.

[10]
http://www.websense.com/global/en/ResourceCenter/WhitePapers/p2p_security.php
File-sharing networks are unregulated and files that claim to be music or movies may contain any number of types of content. This site refers to security threads of peer to peer networks throughout a company's environment. Explains how business enterprises are becoming aware of the many risks involved with employee use of p2p applications.

[11] Panko's Business Data Networks and Telecommunications,
Chapter 9,5th Edition
Copyright 2004, Prentice Hall

[12] http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-2p/html/AS04.html
This report surveys peer to peer content distribution technologies, aiming to provide a comprehensive account of applications, features, and implementation technologies. Defines the basic concepts of peer to peer computing and present the main attributes of peer to peer content distribution systems and their aspects of their architectural design.

[13]Computer System and Network Security, page 144-146
Gregory B. White, Eric A. Fisch, Udo Wr. Pooch
CRC Press

[14]Shane Balfe, Amit D. Lakhani, Kenneth G.Paterson
Trusted Computing: Providing Security for Peer to Peer Networks
Proceedings of the Fifth IEEE International Conference on Peer to Peer Computing (P2P'05)
2005 IEEE

[15]http://www.ece.rutgers.edu/~parashar/Classes/01-02/ece579/slides/security.pdf
This paper has surveyed some security issues that occur in peer to peer networks, both at the network layer and at the application layer.It shows how techniques ranging from cryptography through redundant routing to economic methods can be applied to increase the security, fairness, and trust for applications on the peer to peer network.

[16]http://www.webopedia.com/DidYouKnow/Internet/2005/peer_to_peer.asp
This site explains how authentication, authorization, and encryption help establish trust between peers in a Peer to Peer application. Moreover, it is described a mechanism based on digital signatures, so as it can be clear how the content exchanged between peers can be validated. Furthermore, enumerates the elements of a peer to peer trusted network.

[17]http://www.webopedia.com/DidYouKnow/Internet/2005/peer_to_peer.asp
General notes about peer to peer networks. Starts with their architecture and compares it with that of client/server's model. Classifies the forms of p2p, according to network and application, as collaborative computing, instant messaging and affinity communities. Explains how peer to peer file sharing clients work and concerns about some security issues.

[18]Network Security Architecture
Sean Convery, CCIE No 4232
page 122-161
Cisco Press

[19]http://www.nortelnetworks.com/solutions/security/collateral/nn108120-051705.pdf
This report describes ways for a secure business environment. Moreover, analyzes the risks and the holes of the security and gives a detailed description of how to create a secure and quality network, using modern technologies. Gives good advice to secure perimeter the business network using multiple approaches and techniques.

[20]http://www.hill.com/archive/pub/papers/papers.asp?yr=2003&mn=03
Refers to the usage of peer to peer in enterprise network. Explains the advantages of such an adoption and compares the model with that of client/server's. Moreover, gives brief information about how the file sharing peer to peer model works, as well as the current business p2p model. Ends with some suggestions for the future.

[21]http://p2p.internet2.edu/documents/What%20is%20peer%20to%20peer-5.pdf
Analyzes the models of peer to peer communications (pure, partial reliance, federated p2p) and explains their applications and propose potential areas where each model can be applied. Articulates some security issues and lists a
few advantages for peer to peer networks. Ends with some ideas for future work that enable internet2 with peer to peer networks.

[22] http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

Refers to the security in peer to peer networks. Starts with the need of security by enumerating the external and internal threats in p2p.Moreover analyze some security mechanisms such as secret key and public key techniques. Furthermore, refers to some authorization protocols that allow peers to o ensure that they are speaking with the intended remote system.

[23] http://www.michigan.gov/cybersecurity/0,1607,7-217--121419--,00.html
This site enumerates the attacks on peer to peer networks,such as poisoning attacks, denial of service attacks, defection attacks, insertion of viruses to carried data, malware, filtering, identity attacks, spamming ect and analyses them. Moreover, provides adequate information for security technologies to help you prevent threads in peer to peer networks.

[24] http://www.sans.org/rr/whitepapers/policyissues/510.php
Refers to peer to peer file sharing networks and their security risks. Starts with the history of file sharing networks by giving a brief description of Napster and continues with more recent file sharing services as Limewire and Kazza. Gives a detailed list of treats in these services and suggests some solutions.

[25]Apostolos Tramantzas Bary M.G Cheetham,Mark van Harmelen,Alexandria C. walker
Peer-to-Peer Networks Based on Hierarchies of Trust
Prossensings of the Fifth IEEE International Conference on Peer to Peer Computing (P2P'05)

[26]E.Damiani, S.De Capitali di Vimercati,S. Paraboshi,P.Samarati,F.Violine
A reputation-based approach for choosing reliable resources in peer- to- peer networks.
Proceedings of 9th ACM conference on Computer and Communications security

[27]http://www.caip.rutgers.edu/~dipankar/Papers/Trust%20and%20Reputation%20Model%20in%20P2P%20Networks.pdf
Refers to trust and reputation in peer to peer networks, defines them and explains their differences and their importance. Furthermore, in this paper, it is proposed a Bayesian network-based trust model and a method for building reputation based on recommendations in peer to peer networks. Bayesian networks provide a flexible method to present the differentiated trust and combine different aspects of trust.

[28] http://en.wikipedia.org/wiki/Friend-to-friend
This site makes an introduction of Friend-to Friend networks.Refers to some current uses of F2F as well as suggests some future uses.Moreover, makes a brief description of what frient-to-friend network is and what is not.Furthermore, expaines some security beaches in those kind of network and suggests their solutions.

[29] http://security.jxta.org/
This site refers to JXTA peer-to-peer security project, Gives a list of certain security intrinsic advantages of peer to peer networks, such as privacy, locality, web of trust and no central point of knowledge. Moreover, gives information about the *Cryptography Toolkit for JXTA Technology and about the* "Poblano - A Distributed Trust Model for Peer-to-Peer Networks.

[30] Dr. Dobbs's Journal, page 22
October 2005