Global Information Assurance Certification Paper

A Review of Peer-to-Peer Network Insecurities in Business Applications
Should you take the Risk

Joanne Kossuth

Peer-to-Peer is a network model in which each computer can function as both a client and a server. Any computer in this network can both receive and transmit data. This model has been around for a number of years and has historically been utilized in small networks and gaming. This is partly due to the fact that all resources in a peer-to-peer network reside on local machines and access to resources is not controlled by a central entity such as a server.

One of the major insecurities in this type of network is that each individual user is responsible for controlling access to the resources located on his/her machine. Each user is thus a possible single point of failure. Windows 98 is a commonly used operating system in peer-to-peer networks. In Windows 98 machines, resources are shared through the following procedure:
Click on Control Panel;
Double click Network;
On the Network Properties box, select file and print sharing ;
To grant access, select the "I want to" options;
Click okay and the reboot.
Once the computer reboots, create a share by selecting the folder via My Computer or Explorer and right click on the folder.
Click sharing, share as and enter a name for the share;
Grant read only or full access as desired.

At this point, the system allows you to password protect the share. Please note that since only a password and not a username is required, as long as a user knows the password he can get the level of access that has been granted. If a user shares the password with others or if the password is discovered via shoulder surfing, social engineering, etc the user has breached the security. In addition, if the user with the password (permissions) leaves their computer unsecured (logged in and not screen saver/password protected at a reasonable interval) anyone can gain access to the information stored on the local computer since the operating system will not require a password for shared local folders.

Another vulnerability involving the setup of shares in the aforementioned Windows 98 systems deals with the directory structure. If an entire folder is shared then any subfolders beneath the shared folder are also shared. Shares are not aware of the existence of other shares therefore any overlap of shares within the directory structure will result in additional security holes which breech the confidentiality of information and have the potential to degrade the integrity of the information.

A suggested solution to the sharing vulnerability is to hide shares by appending a dollar sign ($) to the end of the name of the share. This results in the share not being visible through Explorer or Network Neighborhood. However, even a novice user has the ability to map drives and once the share name is known or propagated via any number of methods this "security through obscurity" does not provide much, if any protection.

A "feature" of Windows 98 offers the option of caching passwords. This creates another security vulnerability in that the operating system creates a .pwl file on the C: drive which will correspond to the username. Therefore, if that file was compromised, the hackers could obtain the password tied to your username and/or copy the file and then be able to log in and gain access to all of your shares.

Due to these and other limitations and vulnerabilities, these types of networks fell into relative disuse with the advent of more centralized client/server computing. Within the past year, in particular, P2P (peer-to-peer) networking has made its way onto the Internet. At first, this type of networking was defined by programs such as Napster and Gnutella. In fact, these programs are just the beginning of a new paradigm. Many businesses are starting to explore the "benefits", especially the perceived "cost benefits" of P2P computing. According to Robert Batchelder of Gartner Dataquest there are currently over one hundred businesses testing P2P applications such as collaboration, sharing, and research. Given this new business focus, one has to question whether or not the information security considerations have been adequately evaluated prior to the deployment of the technology.

The business focus in P2P computing can be broken into two technologies. One focuses on sharing processing and storage between different computers (distributed computing) and the other focuses on sharing files, data, video, etc between different computers (file sharing).

One example of the distributed P2P computing model is DataSynapse, which has targeted the financial services market. This company is creating a computer network from home computers that will be able to serve as virtual computing power for DataSynapse's clients. Each computer owner is required to download proprietary software. When the home computer is not processing, the proprietary software will take a portion of the DataSynapse load from the DataSynapse server, perform a process and then return the results of that process to the Company. The home computer owner is paid a fee for processing time. DataSynapse personnel believe that providing their clients with speed measured in minutes as opposed to hours will allow the decision making process in the financial industry to be closer to "real time". Another example is Entropia, Inc., which is assisting scientists working at Scripps Research Institute by linking them to large numbers of PC users for an AIDS project. Entropia takes a portion of the accumulated processing power and sells that to firms that would normally need to rent high-powered computers.

Parabon Computation of Fairfax, VA utilizes its Frontier program to distribute tasks to provider computers running their proprietary Pioneer compute engine software. Results of the computations are sent back to the Frontier server and the clients collect the results at their leisure. Nomad research is an early customer. Nomad found that jobs that previously took weeks to run now run in hours due to harnessing the power of multiple provider computers.

The first possible vulnerability is the requirement to download proprietary software. The download must be checked for known viruses, especially Trojans and worms. There is also the possibility of an availability attack in which the client could be pointed to "fake" distribution server. The client would then download a version of the software that had been altered in a way to benefit the attacker, who could be anyone including a disgruntled employee, a competitor who has used social engineering or other means to gain access to the information on the "out processing" or a student intern. A second major security vulnerability in this type of implementation is allowing third parties access to proprietary information. Once the data is sent from the server the owner of the data no longer has control over that information.

Although the proprietary software recognizes when the home computer is idle and then begins to process, it does not preclude the ability of the system owner to execute other tasks at the same time that may have a negative impact on the data being processed. The system owner could also write a program to intercept or copy the data during its process and thus attack the confidentiality of the information. If the system owner programmed an attack to change some of the information in the data packets then the system owner could attack the integrity of the data as well.

The system owner is not the only threat. In peer-to-peer networks there is a dependence upon the owner. However, most owners either do a default install or purchase their computers with a default install included. The default install maximizes available functions and often does not require passwords or privileges to perform most actions (or has passwords such as "default"). These facts expose the owner's system to vulnerabilities, which can be exploited by others on the network. This is especially of concern with regard to the cable modems, which are "always on". In addition, the lack of a secure, encrypted connection can make the information vulnerable to a "sniffing" attack, which would attack the confidentiality of the information. If you were in a highly competitive business the number of ways in which your competitors could gain competitive intelligence about your company has just increased.

An example of the file sharing P2P computing model is workgroups using the network to exchange marketing, product design, publication and other information. Although this technology is appealing in that it may reduce some of the administrative burden it also reduces security and related administrative controls. Groove Networks is an example of this type of technology. Groove software is comprised of a free 10-MB client. The client allows users to access instant messaging, voice chats, file sharing, threaded discussions; web browsing, and drawing (free-form) as well as video. With Groove, all information is

a file stored on each computer in the peer-to-peer network, purportedly in encrypted shared spaces. When changes are made in one computer all of the computers are automatically updated. When a user accepts an invitation to join a share (through e-mail) the server automatically distributes and installs the code. No passwords or usernames are required for users to exchange information. Groove purports to maintain some central administrative control through the ability to set policies from a console. Transparent storage services store user actions in a secure XML object store, on the computers themselves. Alliance Consulting is one of the early Groove customers. Alliance is building the following applications using the Groove platform:
An application to support distance based learning in the sports industry;
A shared workspace application for supply chain management; and
Applications to roll out new products at various financial services corporations.
Alliance has an application called "Peer-to-Here" which it has trademarked. This application has a proxy that acts as an agent to provide a connection to services outside the Groove space.

As in the case of the distributed model, the first possible vulnerability is the requirement to download proprietary software. The download must be checked for known viruses, especially Trojans and worms. There is also the possibility of an availability attack in which the client could be pointed to "fake" distribution server. The client would then download a version of the software that had been altered in a way to benefit the attacker, whoever that might be. Another vulnerability is the fact that the product has yet to have its first commercial release (due the end of the first quarter). The preview version has not yet had enough exposure to allow for the "bugs" to come out. For instance, many P2P sharing applications leave IP addresses behind. This results in a loss of privacy for users who believe they were operating in an anonymous manner. A critical issue for potential clients is the need to integrate back-end business systems such as Oracle, SAP, etc which contain confidential business information. Encryption levels become key in providing higher security levels.

Another major security concern deals with the omnipresent IP infrastructure. Once peer-to-peer networks are deployed running programs such as Gnutella and Groove, the peers or computers no longer require DNS services. These computers do not need servers to work. The P2P applications have found their way around DNS addressing by assigning specific times for specific nodes to contact fixed IP directories and by designing directories that can update IP addresses in real time.

Dan Kegel discovered a work around for setting up peer-to-peer networks while dealing with proxy servers and NAT (Network Address Translation Protocols). If a NAT is configured to allow incoming traffic from an outside address only if an outgoing packet has already been sent to that address then theoretically two computers behind two different NATs will not be able to open connections to each other. Dan used a method whereby all old peers send a UDP packet to the new peer and the new peer sends a UDP packet to each of the old peers. The first packet is always sent to both the public and the private addresses since the peer computers will not be aware of which NAT they are behind. NAT then opens up a bi-directional hole for UDP traffic to go through. Once the

reply comes back from the peer the sender knows which address to use and can stop sending packets to the other address. The bottom line is that proxy servers and NAT will not prevent the P2P applications from appearing on your network.

A hybrid P2P architecture that has been discussed is one in which a server is located behind a firewall. This type of setup will technically allow for in-house computers to be peered while controlling peers outside the enterprise. WorldStreet Net is one example of this. In the case of American Century, a three-tier security system is in place requiring three levels of logon that can be blocked or opened to the sell-side peers at the company's discretion. The passwords are currently stored on servers that are located at World Street but the company is planning to bring those servers in house. Levels of encryption along with eliminating the servers as a single point of failure will be important factors in the success of the P2P project at American Century.

The hybrid architecture is also important in that the majority of P2P applications lack management tools. The lack of these tools along with other scalability and security concerns results in P2P applications being described as difficult to effectively integrate into an enterprise infrastructure. The hybrid model has the ability to provide some of the management functionality. The Peer-to-Peer Working Group (Intel, IBM, etc) has been working on developing technical requirements, which include persistence, accountability, fault tolerance, exception management, scalability, and resource discovery and management.

CO by Oculus Technologies Company is one of the latest peer-to-peer tools. CO is similar to Napster but is designed to handle large size files such as CAD and other engineering applications. In order not to expand storage requirements exponentially, CO shares only a "black box" of each model. Users get to view details only as required. This method also improves the security of the application compared to other P2P technologies. The entire original model remains on the person's machine that created it. Even if an encoded message were compromised, the user would see only a small portion and not the entire model. This type of data sharing is referred to as "granular". The tiny shared packets also result in faster sharing of information as required (even over dialup connections). According to Christopher Williams, President and CEO, "CO is not meant to replace current engineering software tools but to enhance them, enabling them to collaborate". Oculus utilizes 128-bit encryption but currently has a high price tag; $5000 per user.

P2P technologies are definitely here and the applications will be coming fast and furious. The pressure will be there to buy fewer "servers", store less data centrally, employ fewer people, reduce office overhead by allowing more employees to collaborate remotely, reduce or eliminate standard fax and e-mail transactions and applications, etc. Businesses will need to do a thorough risk assessment of their enterprise prior to deploying P2P technologies. Only after questions such as what is being protected and how valuable is it to the company or to others are answered can a company make an appropriate decision with regard where and when to utilize P2P technologies. Once that decision is made there will still need to be sufficient planning for in-depth defenses including monitoring.

References

Ames, Benjamin B. "A new way to CO-llaborate". Design News. 23 January 2001. URL: wysiwyg://1884/http://www.manufacturing….agazine/dn/dntoday/jan2001/12301ames.html

Contributor, Guest. "An introduction to peer-to-peer computing". TechRepublic. 27 December 2000. URL: wysiwyg://11/http://www.techrepublic.com…ABOWSCTEAALSFFA?

Eweek Reporting. "P2P: Coming to an enterprise near you". EWeek. 12 December 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2664986,00.html

Gilbert, Alorie. "Peer-To-Peer Makes for Speedy Design". Informationweek.com 29 January 2001. URL: http://www.informationweek.com/maindocs

Harrison, Ann. "Today's Focus: Crunching data from the ionosphere ". Network World Newsletter. 01 February 2001. URL: http://www.nwfusion.com

Harrison, Ann. "Today's Focus: Into the P2P groove ". Network World Newsletter. 08 February 2001. URL: http://www.nwfusion.com

Harrison, Ann. "Today's Focus: Groove client develops P2P business apps". Network World Newsletter. 13 February 2001. URL: http://www.nwfusion.com.

Kegel, Dan. "NAT and Peer-to-peer networking". 17 July 1999. URL: http://www.alumni.caltech.edu/~dank/peer-nat.htm

Kwan, Joshua. "Peer-to-peer promises to reshape the Net". Silicon Valley News. 12 February 2001. URL://wysiwyg://1650/http://www0.mercurycenter.com/svtech/news/topdocs/peer021201.html

Nichani, Maish and Rajamanickam, Venkatesh. " November Special Report: Deconstructing "Groove"". Elearningpost. November 2000. URL: http://www.elearningpost.com/elthemes.groove.

Oculus Technologies. URL: http://www.oculustech.com

Oram, Andy (Ed.). "Peer-to-Peer Harnessing the Power of Disruptive Technologies" 13 February 2001. URL: http://www.oreilly.com/catalog/peertopeer/chapter/ch01.html

Peer-to-Peer Working Group. "Welcome, First meeting" (Powerpoint presentation). Intel. 12 October 2000.

Posey, Brien, M. “Security on a Peer-to-Peer Network”. TechRepublic TechProGuild. 17 August 2000. URL: wysiwyg://78/http://www.techrepublic.com…rfriendly.j.html?

Vaas, Lisa. “P2P ascends to new prominence”. EWeek. 17 December 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,2663716,00.html

Vaas, Lisa. “P2P gets jury of its peers”. EWeek. 18 December 2000. URL: http://www.zdnet.com/eweek/stories/general/0,11011,26637115,00.html