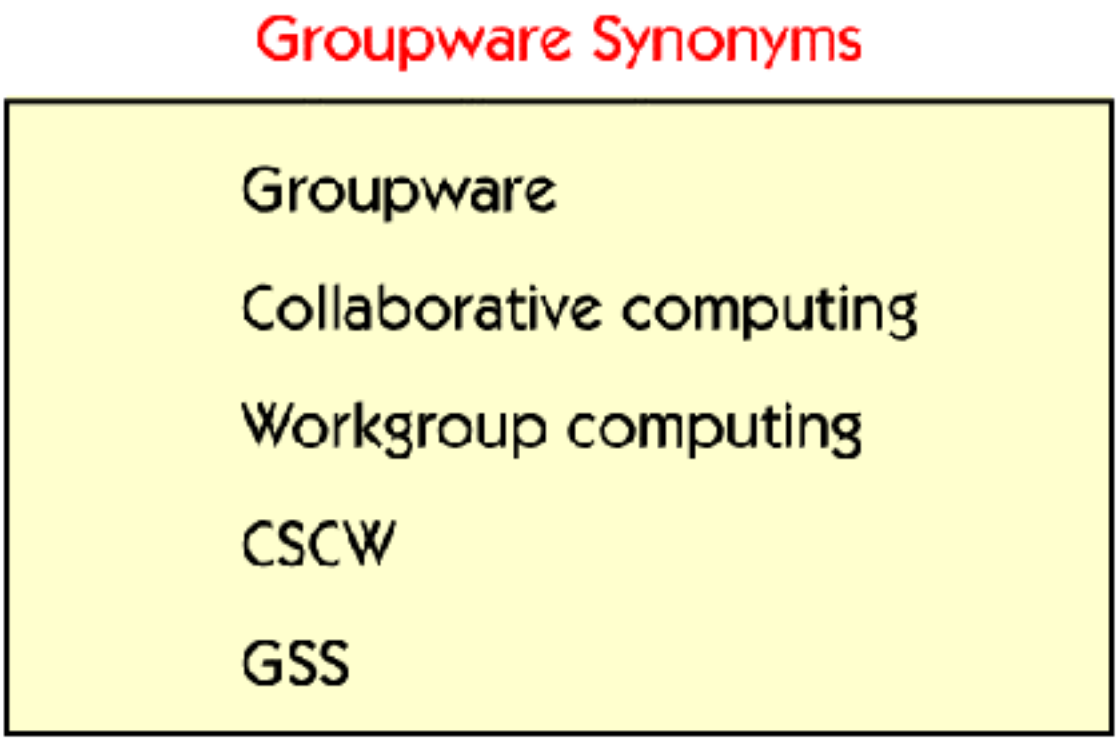
Ch.10 - Groupware & Security



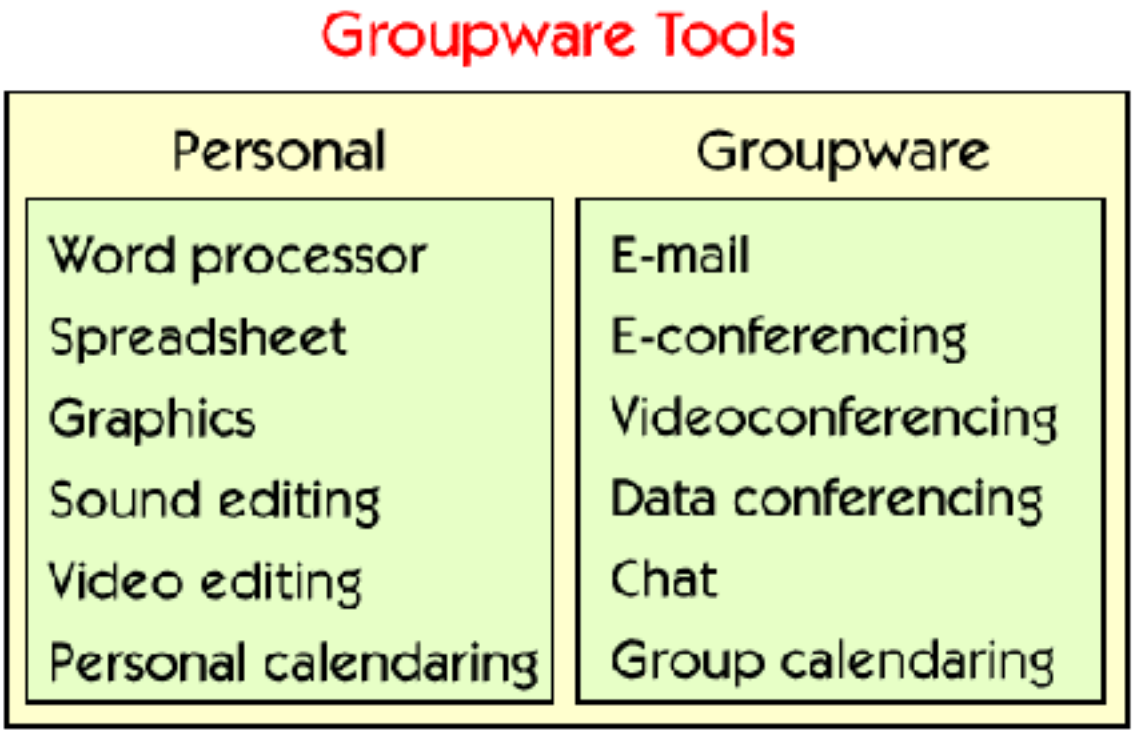
People use different terms for groupware. The following words are frequently used:
- Collaborative computing.
- Group computing.
- In the academic world the term CSCW, which stands for Computer Supported Cooperative Work, is often used.
- You will sometimes see GSS, which stand for Group Support Systems.

All these terms refer to the same thing, but groupware is most commonly used.

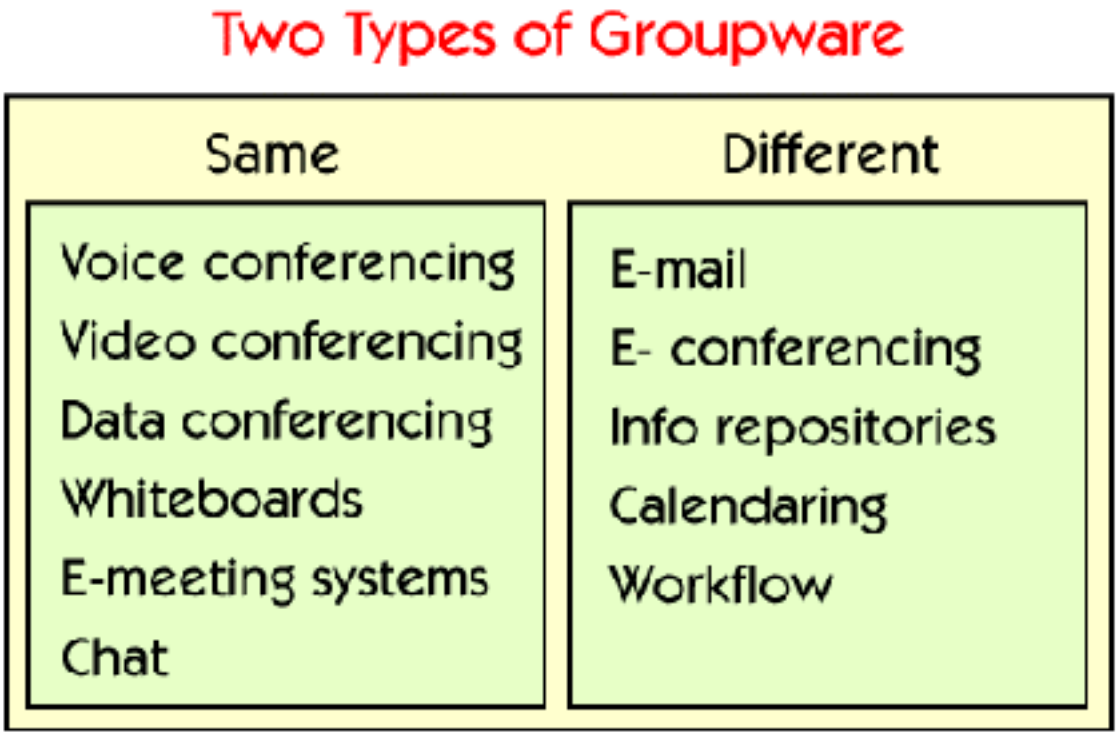
Definition of Groupware

A tool that helps people work together more easily and more effectively. It allows them to communicate, coordinate and collaborate.

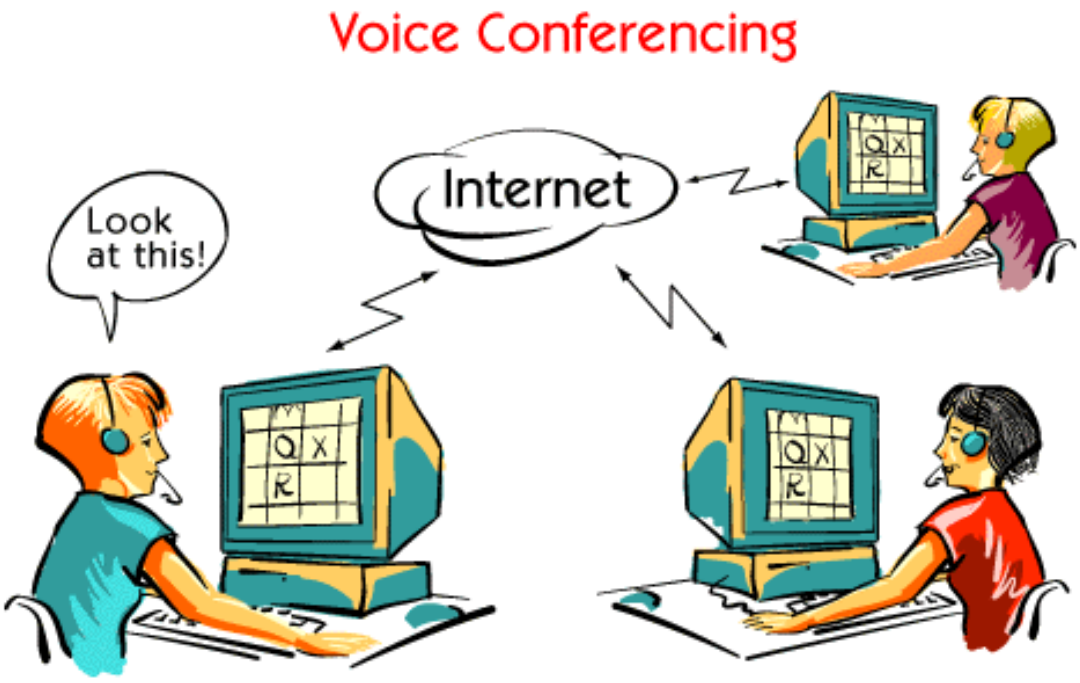
Groupware is a tool that helps people to communicate, coordinate and collaborate. Well, if that is the definition then you could argue that a normal telephone is groupware.
That is not so. When people speak of groupware they mean a computer based tool. So normal telephony is not considered groupware, but Internet telephony is.



There are two kinds of software based tools. Personal tools and groupware tools. Personal tools, like a word processor, spreadsheet or a video editing program are used by individuals. Groupware tools on the other hand are always used by several people. E-mail, voice conferencing and chat are typical groupware tools, since it's only meaningful to use them for communicating with other people.

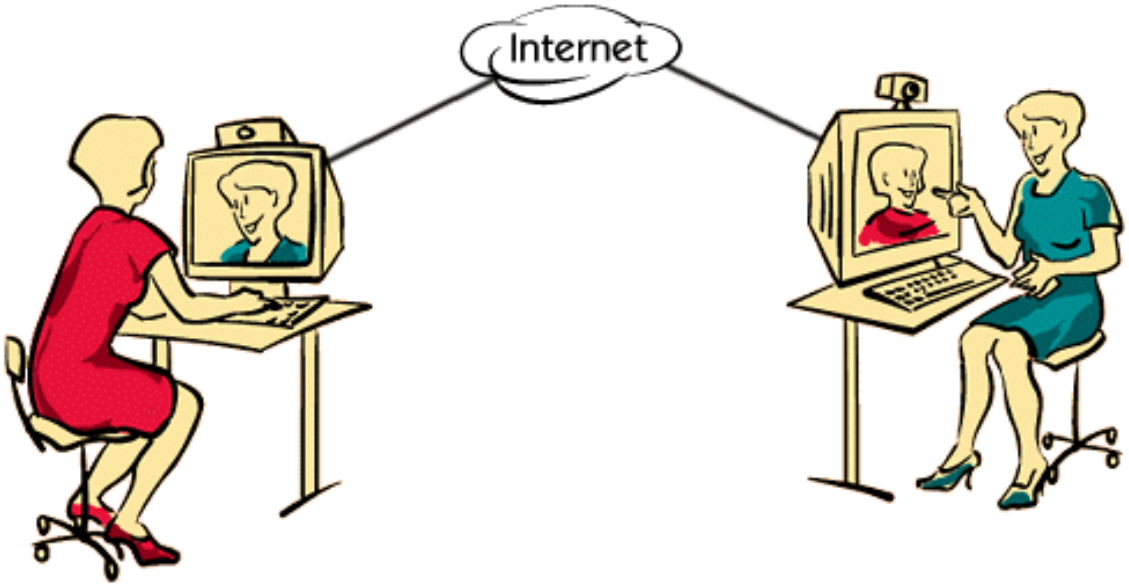


Some groupware tools are used for synchronous communication, while others are used for asynchronous.
Synchronous communication requires that all parties are present at the same time. Typical examples are voice conferencing, video conferencing and chat.
In asynchronous communication the sender and receiver can operate at different times. E-mail is a typical example; You send a message at one point in time while the receiver reads it at another point in time. Other examples are electronic conferencing like Usenet news or group calendaring.



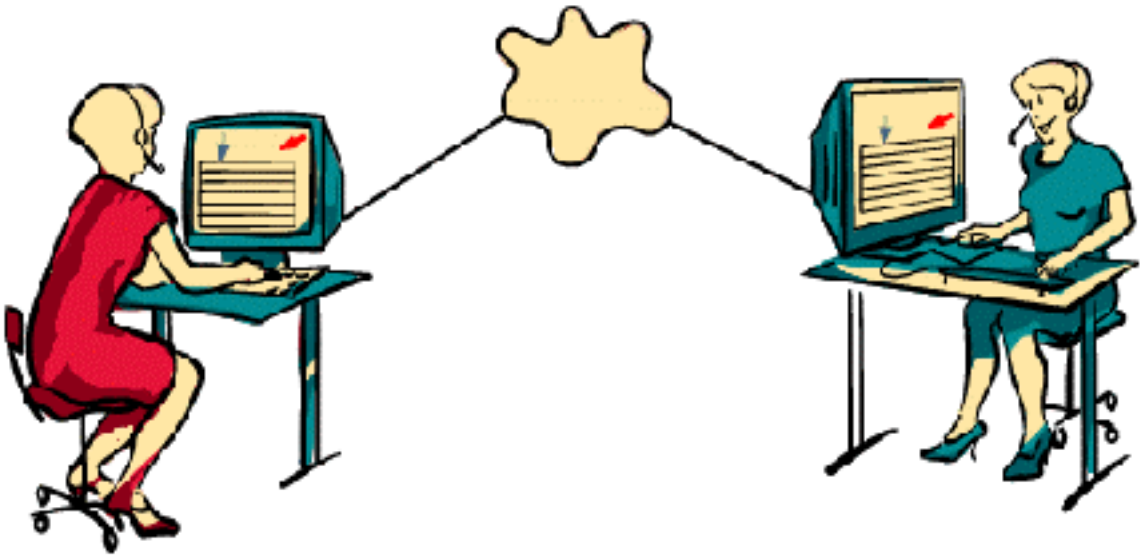
Voice conferencing allows people located in two or more places to speak to each other.
Traditional voice conferencing tools consist of speakerphones and telephones.
Computer based voice conferencing consist of Internet phone tools that normally also include chat and whiteboarding. Many computer based voice conferencing tools can connect multiple locations.
Computer based voice conferencing is a bit confusing at first due to time lags and participants have to get used to the situation.
The most known tools that include voice conferencing are CoolTalk, NetMeeting and CU-SeeMe.

Video Conferencing

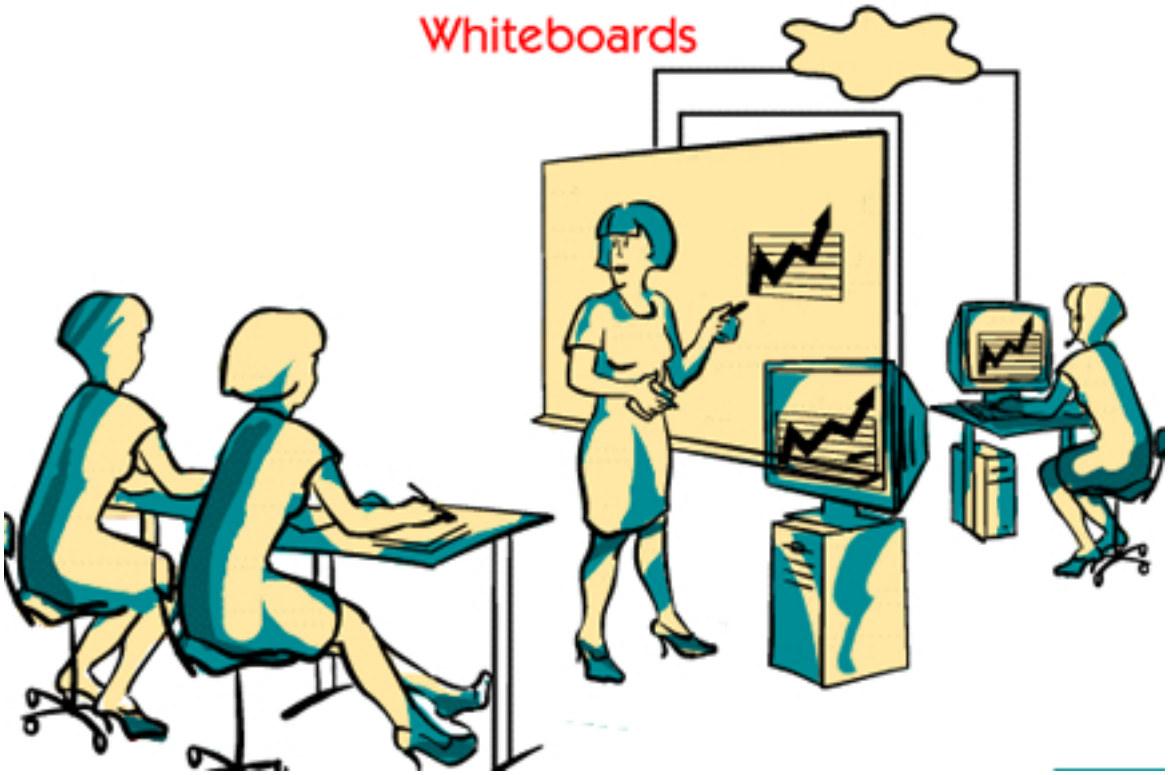


Video conferencing allows people at different locations to see and hear each other. A video camera captures pictures while a microphone captures sound. Both these signals are digitized and sent over telephone lines.
Video conferencing comes in two flavors. The first one is used in special conference rooms. The quality is high since high bandwidth is used, but it's rather expensive.
The second one is desktop video, where you can use cheap cameras for about 200 US Dollars and a 28.8 kbps modem. The problem with this kind of cheap desktop video conferencing, is that the quality is low and motions are very jerky. Still you get a sense of presence which you don't get with voice conferencing.
CU-SeeMe was the first application that offered video conferencing over Internet, but now it is also offered by CoolTalk, NetMeeting and others.
Many video conferencing tools also have Whiteboard and document sharing capabilities.

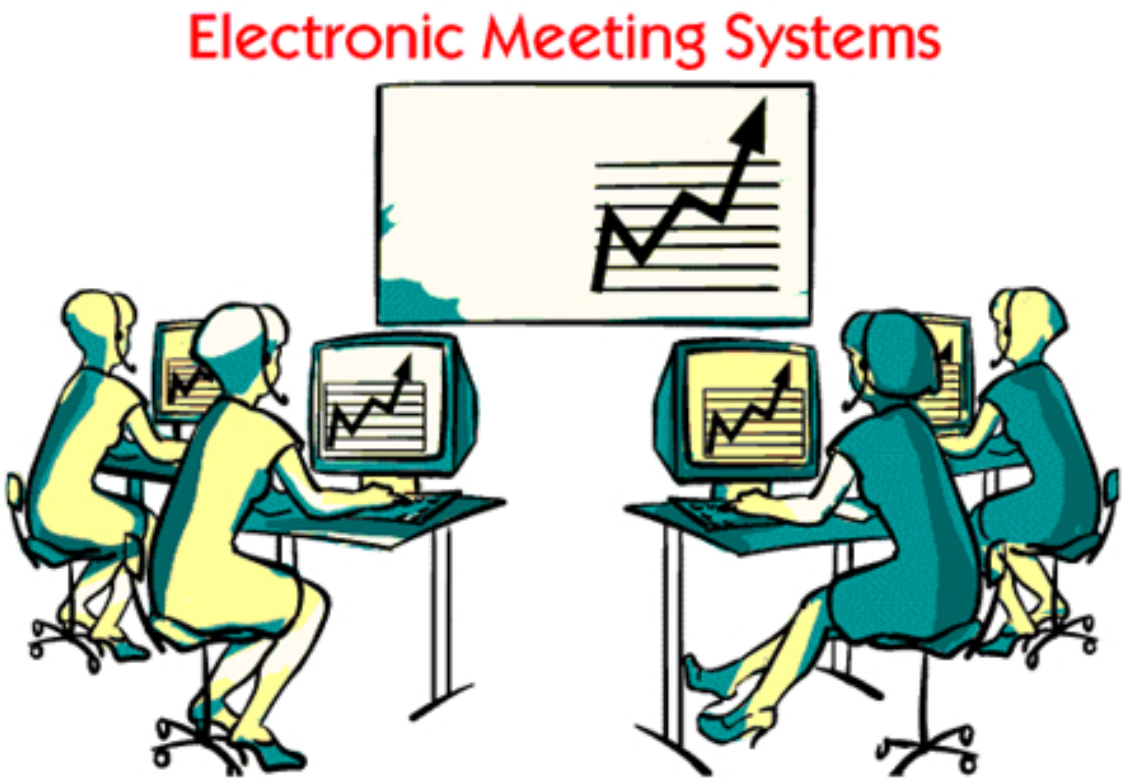
Data Conferencing



Data conferencing lets two or more persons share documents. The persons can simultaneously point to and change a document.
Data conferencing combined with voice conferencing is a very powerful way of communicating.
NetMeeting and Timbuktu are two good Data conferencing tools. Of course there are many others.

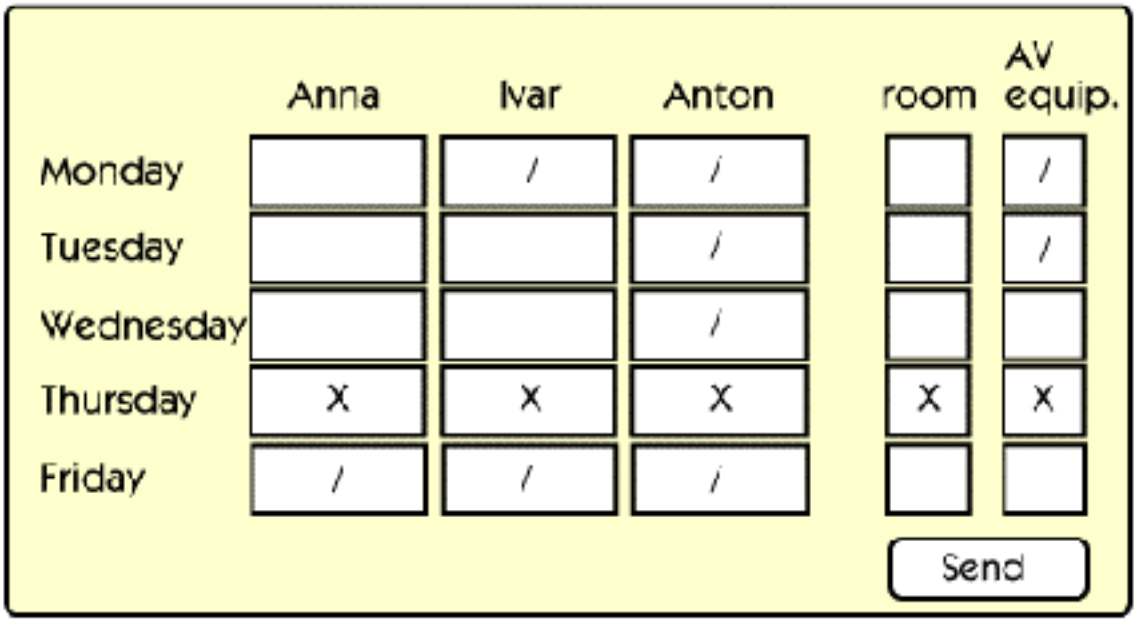


Whiteboards are often used in conference rooms. Everything you write on a whiteboard is captured by a computer and sent to participants at other locations.
There are sensing devices attached to the whiteboard which sense what color of pen you are using , or if you are erasing something. The result is that a person sitting at another location sees a picture on his screen which is identical with the one on the whiteboard.



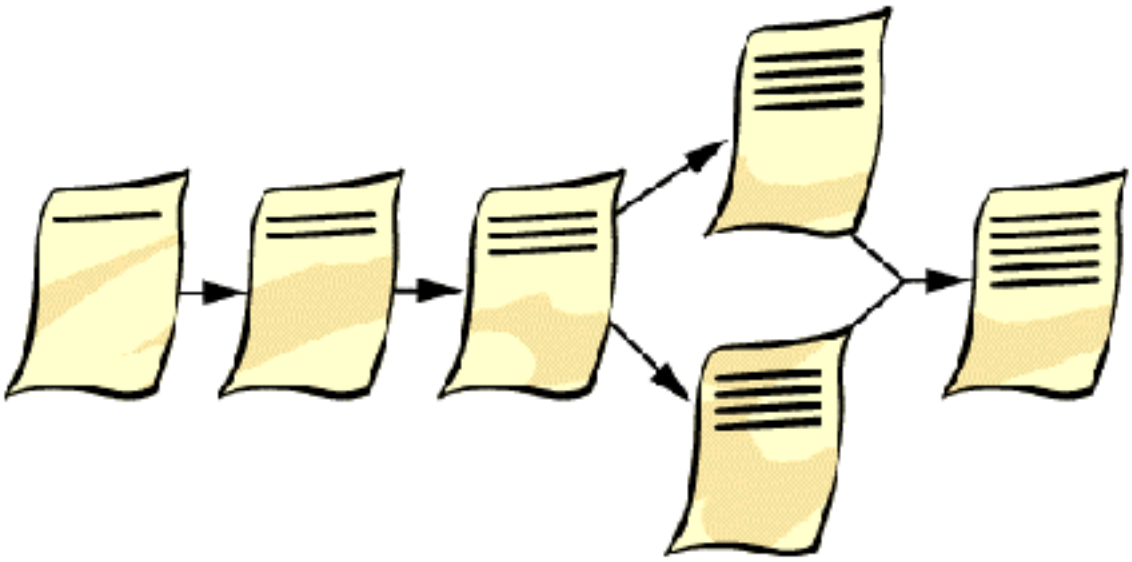
An electronic meeting system uses computers to connect participants in a meeting so they can share ideas simultaneously. Every participant uses a computer that is attached to a large computer screen in the front of the room.
Electronic meeting systems are often used for brainstorming. One advantage is that participants can contribute ideas anonymously, expressing their true opinions.

Calendar Systems

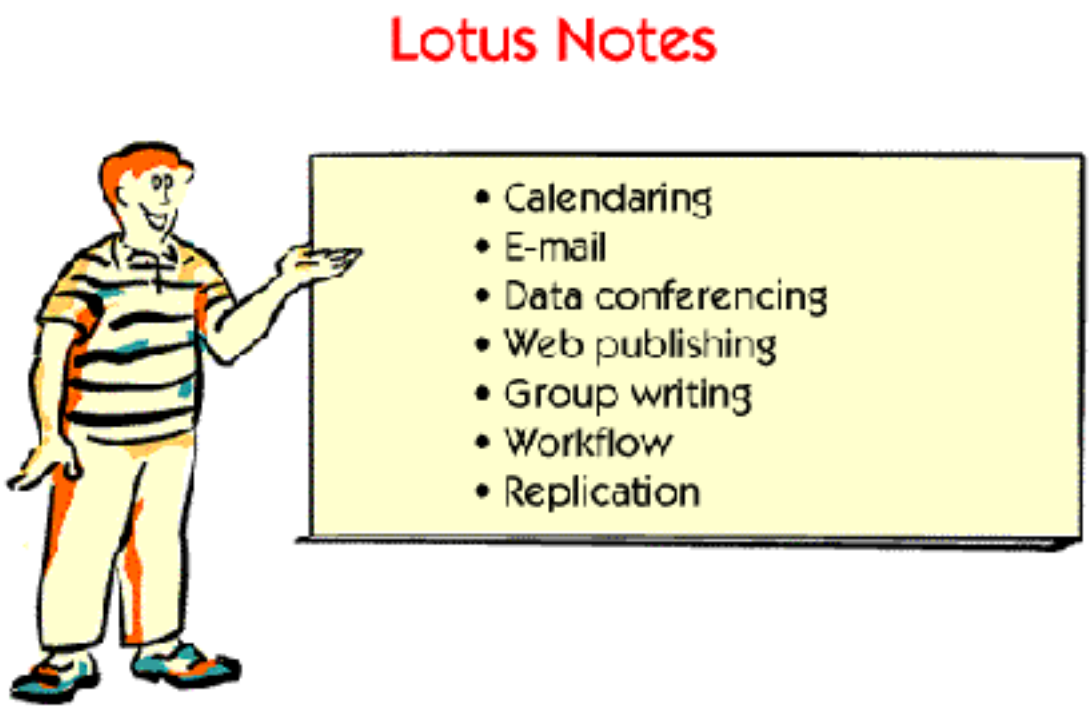


The purpose of a calendaring tool is to make it easier to schedule meetings.
With a group calendar you can see other peoples' calendars. You can select a suitable time for the meeting and book resources like conference rooms and equipment. A notice will then be sent by e-mail to each participant, asking for confirmation.
Some groupware tools that include calendaring are Lotus Notes, Microsoft Exchange and GroupWise.

Workflow



Workflow tools let you work with documents that are processed in a series of steps that change the state of the document. When the state of the document changes the persons involved are notified, for instance with an e-mail message.
Teams that are developing products often use workflow tools for project and task management.



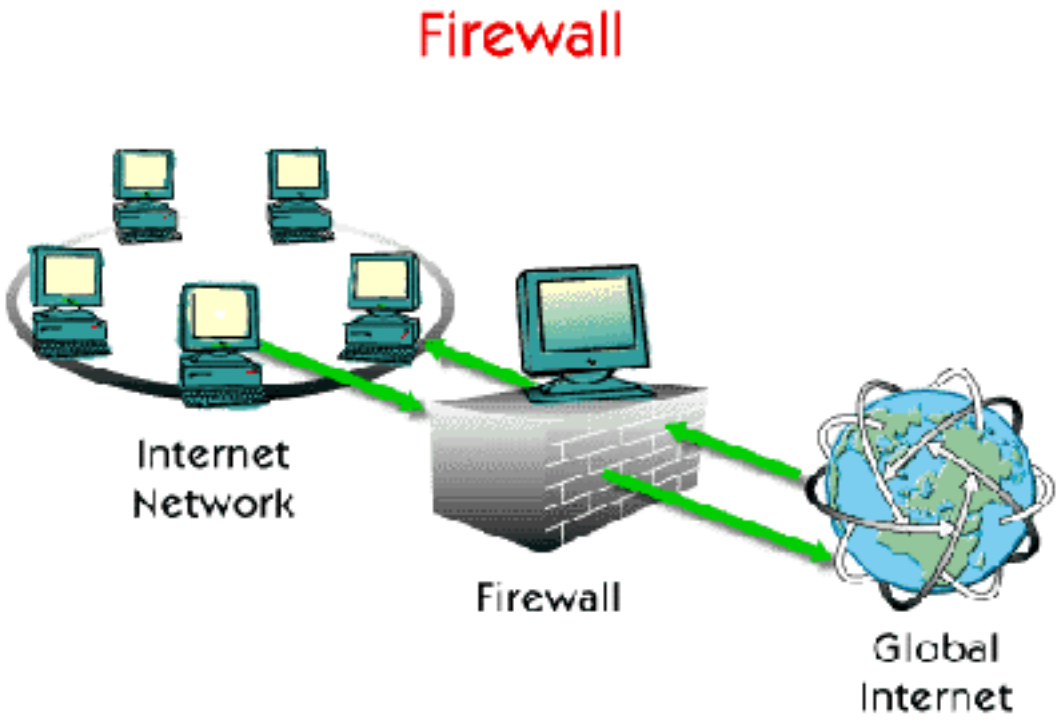
Lotus Notes came out in 1989. Because Lotus Notes was ahead of its time, many people think of Lotus Notes when they think of groupware.
Lotus Notes provides functions for calendaring, e-mail, conferencing, web publishing, group writing, workflow and more.
One of the advantages of Lotus Notes is the support for replication. Replication is the process of duplicating and updating data in multiple computers, some of which are permanently connected to the networks, while others, such as laptops, are connected at irregular times.
In the pre Lotus Notes days, networked databases were stored in one place. Everyone who wanted to access information in a database needed to be physically connected to the network through some form of phone line.

Then along came Lotus Notes whose claim was that everyone could create their own database and carry it with them on their laptops. Everyone could put their own information in and out, and Lotus Notes would update both the central databases and everyone's private database every time they logged into the network**.**

Security

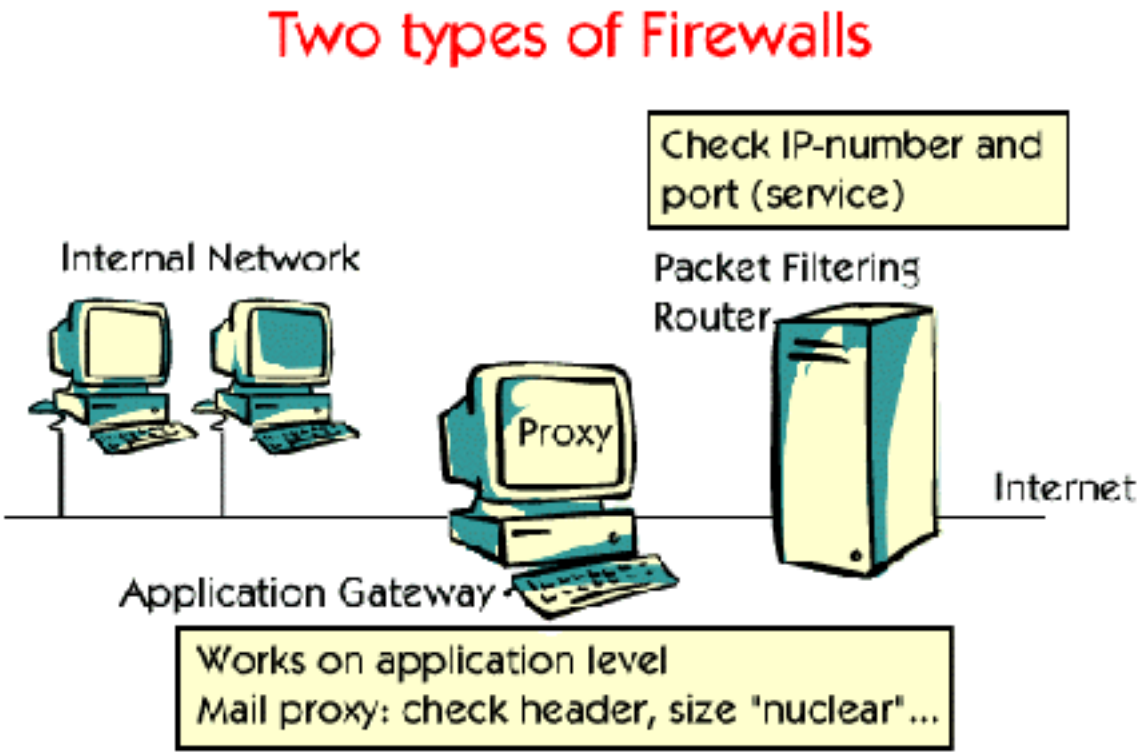
Hacker	To test security system; Steal data.
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company.
Con man	To steal credit card numbers for sale.
Spy	To learn an enemy's military strength.

Two decades ago computer networks were primarily used to share printers and files between corporate employees. There was no need for security. Nowadays computer networks are used for banking, shopping and sharing information with millions of people. Under these conditions network insecurities can mean serious trouble.
Security problems are caused by unauthorised people. A hacker might want to make free telephone calls, a businessman might want to see competitor's offer for a certain job, an ex-employee might want to get revenge for being fired, an accountant might want to embezzle money, a con man wants to steal credit card numbers and a spy might want to steal military secrets.

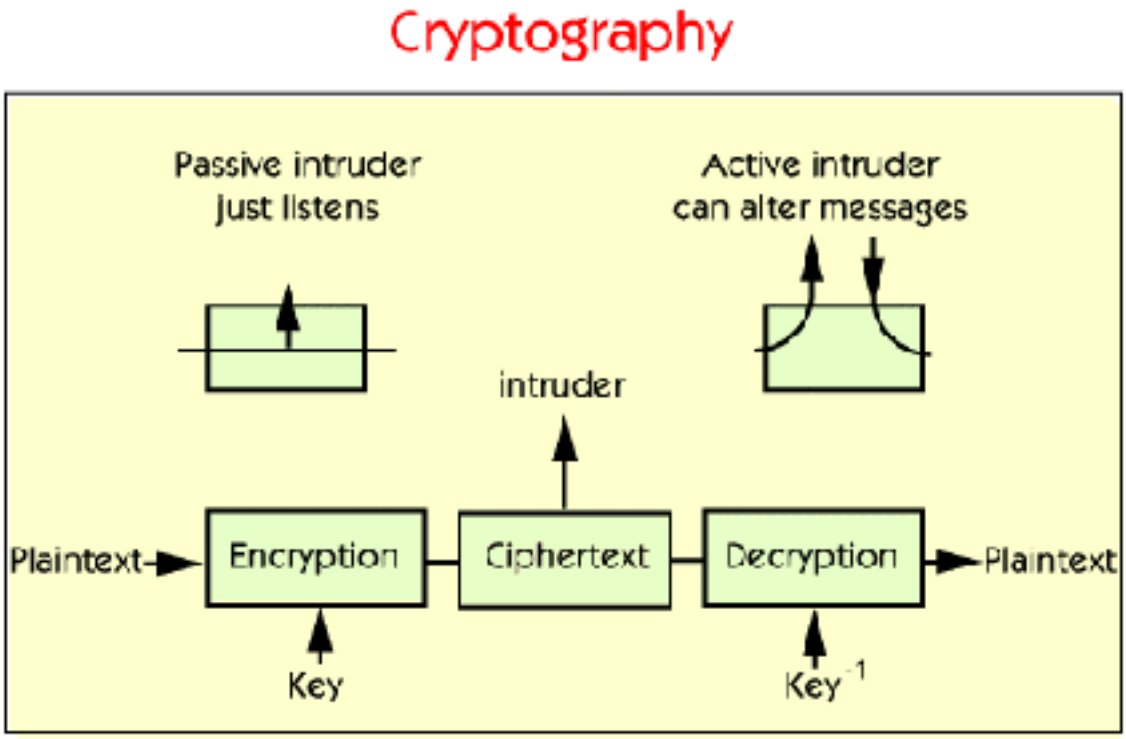


A firewall is a barrier between your company's network and Internet, through which only authorized traffic can pass. As traffic passes between your network and Internet it is examined by the firewall.

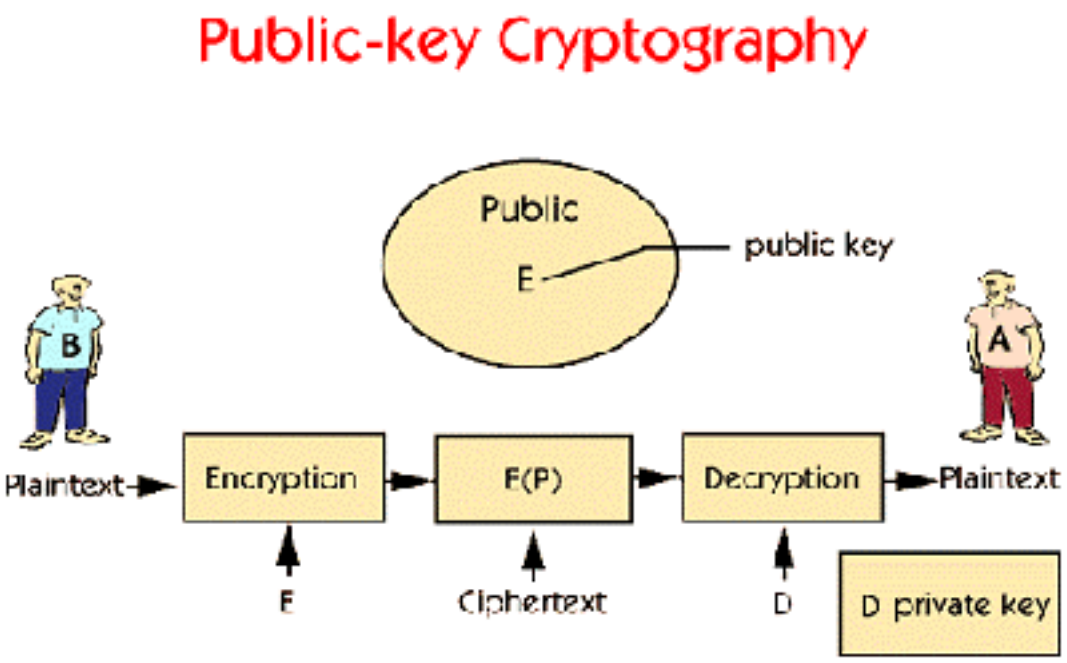
Firewalls are modern equivalents of the medieval castle strategy: Digging moats around the castle and forcing everyone to enter and leave over a single drawbridge, where they can be inspected by the I/O police. Nowadays these I/O police are called firewalls and they normally follow the strict guideline of "whatever is not expressly permitted is denied".



There are two types of firewalls: Packet filtering routers and Application gateways. A router can check every incoming and outgoing packet. All packets that fail the test are dropped.
A packet filtering router checks the IP-number and the port number of a packet. Only certain IP-numbers, like the ones coming from the company's network are allowed to pass. From the port numbers the requested services can be deduced. In this way one can allow some services, like e-mail, but stop others, like telnet.
An application gateway doesn't look at the raw packets; instead it operates at application level. A mail gateway can examine different parameters like message size, header fields and content. Depending on the rules which are set up by the system administrator, some mail messages will be allowed to pass, while others will be screened out.
An application gateway can act as a proxy server. A proxy server acts as a go-between between your computer and the Internet. There are several reasons for using proxy servers.
1. By using a proxy server you can hide internal IP-numbers from the outside. In this way you can make it harder for unauthorised people to configure their computers so they look as though they are coming from inside the company's network.
2. By using a proxy server you can have more computers inside your company than the number of IP-numbers that are assigned to the company.
3. A proxy server can cash pages that pass through it. When a user asks for a page that the proxy already has in its cache it is delivered thus reducing the waiting time and communication costs.
4. An organization often uses a proxy server to prevent employees from having full Internet access. Users talk to proxy server, but it is the proxy server that contacts remote sites on behalf of the client. This mechanism is used for instance to prevent the users from accessing services like RealAudio which could take large portion of the available bandwidth, thus slowing down the network for the rest of the users.



In cryptography, the message that needs to be encrypted is known as plaintext. The output of the encryption process is known as ciphertext. If an intruder hears and copies the ciphertext he cannot decrypt the ciphertext easily if he doesn't have the decryption key. An intruder that can only listen to messages is called a passive intruder. An intruder that can modify messages and inject his own messages is called an active intruder.



Key distribution has always been the weak link of traditional cryptography. Everybody took for granted that encryption and decryption keys were easily derived from each other. Since a key had to be distributed to a user before an encrypted message could be sent to him, there was an inherent built-in problem.
In 1976 two researchers, Whitfield Diffie and Martin Hellman, at Stanford proposed a radically new kind of encryption technique. The idea was two have to different keys, one for encryption and one for decryption, where the decryption key could not be derived from the encryption key. Since the decryption key can not be derived from the encryption key, the encryption key can be made public. This method is called "Public Key Cryptography" and works like this: when B wishes to send a message to A, he looks up A's public key E, for instance on a web page, and uses it to encrypt his plaintext into a ciphertext E(P). He then sends the ciphertext to A. A then uses his private key D to decrypt the ciphertext and reads it.
The difficult thing in public key cryptography is to find an encryption and decryption algorithm so that it is extremely difficult to derive the decryption key from the encryption key. The best known algorithm is called RSA and was invented in 1978.
Public-key cryptography takes a lot of compiling power. It is normally only used for sending small amount of information, like the key to be used for traditional cryptography. After the key is distributed, the traditional cryptography is used for sending large amounts of data.