T17 - Vulnerability of networks to intrusion by Isaku Oba

Over the years the increase in digital technology has succeeded in making the internet much more sophisticated beyond the imagination of the people who created the model of today's internet. However, these revolutionary developments in the network have come with significant side effects.

The user friendly environment and the many attractive services the internet offers have been used by many people in developed countries and have succeeded in connecting huge numbers of totally unrelated people who do not even live close to each other. Also still it is these three of the most obvious benefits that have resulted in making our personal information vulnerable towards possible 'thefts' from others.

The first aspect, the connection of many people anonymous to each other has given skilled computer programmers a reach towards personal information. In order to steal personal information without the internet, it is required for the stealer to actually get to the source of the information, but in the internet, the dimension of distance has become almost nonexistent. This is extremely important because without the internet the stealer actually has to come in physical constant to the direct source of information. In this case the stealer leaves a trail behind him, which will allow the victim to find out who stole the information. When we are connected to the internet through our server which contains our personal information, it is like going into a building carrying a briefcase full of our information, making us extremely vulnerable to theft.

It is also impossible to neglect that the internet connecting us to almost all the people in the world will make everyone in connected to the internet, even those who have never met the stealer, or even live on the other side of the world. Therefore if a person can design computer programs which can some how extract information from a 'trap' that lets him view information through our server, he can steal information from anyone, anytime, and anywhere. This raises the ethical issue of the power held by these programmers, which leaves the fate of our information to the ethical values of these programmers. We will have to take more caution in our life using the internet, for example not entering suspicious sites as they may be traps and taking precautions in our email as there might be Trojans inside them.

The vulnerability of personal information obviously does benefit the creator of the technology, the programmers, who may sell the information they gain or use it to create other benefits for himself: but another group that takes advantage of the suffering of normal internet users who fearing loss of information is the network security companies. The internet users will now live in fear of people looking at their personal information. This will cause the demand for programs that prevent this to rise, creating more benefit to companies which make products such as anti virus programs, Trojan detectors, fishing site scanners, and trap searchers.

The internet is a sophisticated technology that connects the whole world together. What we cant forget is that all technology comes with its tradeoffs.

T18 - Ability to implement different levels of access by Raymen Ohmori

Security and permissions are of utmost importance in today's world. If you slap a windows computer down in a public Internet cafe with full permissions, I can bet you that in 2 month's time it will be messed up beyond recognition. An even better bet is that if you sat down a computer with no permission restrictions, but with viewable website restrictions, than people will be looking at those blocked sites in a week's time. Of course, this is only concerning permissions on a Windows PC, but nevertheless, it it the most common type of permission and level of access restriction that you will see in your immediate vicinity today.

A glowing example of the importance (At least to the school and the IT Department) is the ability to implement different levels of access is what happened to the new school computers that were bought last year. At first, people used them fairly well, without any screwing around of messing with the computers, except for the people who started opening the computers and taking the RAM sticks. Since this is not the topic of this essay, I will not go into detail here.

Once the computers were padlocked, these actions stopped, but people because restless. Then, the day of the Internet restrictions came – St. Bernard was installed on the school servers and the viewing of Myspace.com, Newgrounds.com, and porn sites were blocked. There was much grumbling and discontent among the populace, and soon after, the local tech gurus came and hacked the system for the innocent victims of this injustice. Tor, an anonymous proxy program, was installed on the computers facing the wall so that the students may bypass the blocking software.

This happened because of the ability of the students to use a certain level of access. Programs could not be installed in system folders (Program Files and WINDOWS) while logged into a student account, but they could be installed elsewhere, and that is what happened. The ability of the school to restrict access to files was limited - if installing was disabled in all the folders, people would not be able to save word documents anywhere outside an external USB drive (or iPod, etc) and they would not be able to download their files that they sent to themselves.

In addition to being an incredible nuisance, this would almost nullify the purpose of the school computers, which were to help the students do essay work. Therefore, it was impossible to restrict access to that fine a level; or so everyone thought.

It was another defeat for the students when the IT Department implemented program-specific restriction – that is, restricting the level of access students have when installing a certain program; in this case, Tor. The school had a well-developed ability to implement different levels of access appropriately, and the innocent victims of website blocking were foiled in their attempts to regain justice.

However, blocking access to certain levels of a computer is not always a matter of depriving students of YouTube video viewing abilities. Firewalls work by implementing different levels of access inside and outside a computer to different applications. If there was a security flaw in a program, and that program had unblocked access to receive connections, a devious hacker could plant malware in your computer though that program without you even knowing! If you did not have a anti-virus program, and a virus you inadvertently downloaded had access to your whole computer, it could do some serious damage – like deleting your hard drive.

Luckily, Windows has some built-in protection that gives a program a certain level of access and does not let it delete your hard drive, at least not before asking you first. However, Windows is infamous for security holes that viruses can crawl through in order to infect the computer and shut it down every two minutes (This was the ms.blaster virus - the writer has first-hand experiences of its effects). Internet explorer, too, is famous for its holes that impair its ability to implement different levels of access to web applets on your discretion.

Lastly, restricting access is not always good. Some programs need access to system files in order to start and run properly, especially the first time when they set system variables, add registry entries and such. On the writer's computer, the writer had a problem of certain programs starting up and immediately turning off without an error message. However, it turned out that these programs needed access to deeper areas of the computer and the operating system the writer was using gave all programs a low level of access. By allowing the program greater access the first time the program was started, problems could be averted.

Apparently, there was no error message because the operating system owned (read: stopped) the processes of the programs that needed deeper access because they were scratching at the door to the restricted area and were immediately assumed to be malicious viruses.

The writer is not quite as complete in his knowledge of Macs and their functions to implement different levels of access, but Mac users insist that the security of Macs are far superior to Windows PCs. Therefore, we can conclude that if you understand the importance of implementing different levels of access in Windows, then security in a Mac should not be a problem.

T19 - Implications of network failure, for example, banks, transportation, hospitals, schools by Haider

In today’s world, the ability to transfer, share, and distribute information and data is just as important as the possession of data itself. With the development of information technology, substantial amounts of money and effort are being put into research and development of efficient and safe computer networks, allowing faster and more secure data transfers. Recent years, however, have seen several cases of network failure across the globe, often resulting in severe financial damage and/or damage to life.

Before the implications of network failure can be assessed in detail, it is first necessary that the role of networks in modern computing is understood. Even though the nature of the function of networks is simple and straightforward, networks are increasingly being embedded as integral components of many other systems, such as schools, air traffic control, traffic systems, movie booking schedules, and the Internet among countless more.

Although network failures are complicated, their social implications are simple: disaster. Networks are such integral components of important everyday systems that their failures can possibly result in the breakdown of the systems themselves. For example, a large network failure affecting the Internet is bound to bring many important systems, such as online flight booking and live conferences to a halt, impacting major corporations and/or individuals financially. Similarly, a failure in a flight communication network can possibly result in the loss of lives. One recent example of a small network failure resulting in a huge impact on other systems was the failure of a traffic control computer in the UK in 20041. Thousands of passengers were delayed and hundreds of flights in the air were subjected to safety hazards.

The dependency on networks and the inherent social implications of network failures also result in a number of ethical dilemmas. First and foremost, accountability becomes difficult because “who is responsible?” becomes a vague question that is difficult to answer. Taking the example of the British flight control failure, if the failure had resulted in a significant loss of life and irreparable financial damages, no one would have been able to pinpoint exactly who was to be blamed. Many people argue that computer network systems are maintained by people, and it is these people who are responsible for ensuring such networks function smoothly. Others argue that the designers of networks are to be held responsible. Yet, others argue that no one can truly be held responsible for network failures and the only thing that can be done is to employ safer networks.

The largest moral dilemma is still whether society should be so dependent on computers and computer networks, allowing itself to fall vulnerable to computer failures. Many critics of computer networks argue that computers and computer networks are created by people and are hence bound to fail once in a while. Reducing systems' dependencies on computer networks hence reduces the intrinsic risk of network failures destroying entire systems, possibly saving lives and money.

But it all comes down to this: the basic reason why computer networks exist in the first place is because they are efficient. As it is with all technology, there is a risk in dehumanizing networks, but the efficiency computer networks provide have outweighed the risks in experience so far. Instead of having people write letters to communicate across the globe, computers can communicate the same data in a matter of split seconds. Hence, although there is an inherent risk in embedding computer networks into important systems of society, the networks are nevertheless the only reason why information technology has progressed to where it is today, and the only sensible approach to this problem would be to invest more time and money into research and development of safer computer networks systems and ensure that the innate risk of network failure is minimized.

T20 - Implications of Collaboration, Groupware and Data sharing by Chaan Tutlam

Ever since the introduction of the internet for civilian use, rather than strictly only for the use of the government, it has quickly become a means for spreading and enhancing information. When information, product, or software is ownerless, and is openly edited by outsiders without any need for permission, this product becomes the result of groupware, collaboration and data sharing. Groupware and data sharing have accelerated the rate of inventions over the internet, but they also have had social implications as well.

What if software is being developed through groupware, collaboration and data sharing and one person decides to claim ownership to it all of a sudden. Since this software is being developed by bits and pieces of contribution from a lot of people's ideas, who will have the right to claim otherwise. Although the unwritten law agreed upon on data sharing is that no one can claim ownership, can this unwritten law be subject to change? After all, it is an unofficial law.

If that software becomes successful, does the "owner", in other words the original poster of that software have the right to claim ownership? In another scenario, what if the software develops into something malicious such a virus and causes damage to an individual's or a corporation's computers, who will be to blame for this. Will the blame rest on the shoulders of the original poster or everyone who contributed to the software?

What if some group of people are editing the software to change its purpose and direction, does the original poster of the software have the right to say anything about what kind of direction his software should take? These issues affect the society as a whole because if corporation's computers are damaged because of that software created through groupware, the corporation will loose lots of money due to this problem.

The main solution to solve these problems and issues would be for some kind of authority body to separate the products of groupware, collaboration and data sharing from the products produced by copyright. In this way, the problems of groupware and data sharing will be isolated to only that area, and will not mix with legal/patented products. If these two "worlds" do mix, as the scenario given above of software made by groupware damaging corporation computers, then anyone who edited that software should be held accountable. Since the owner, once after posting the original software doesn't have full command of this software, it would only be fair to put blame on the editors of that software.

From this solution mentioned above, another problem arises: how do we figure out and trace the editors of software on groupware. A feasible solution would either be to ask for a traceable username when editing or have some kind of tracing software which can be used to trace and find anyone who edits a particular piece of software. This way, even though not 100% guaranteed to work, can put a little barrier of responsibility on the part of the groupware editors.

In the case of the original poster all of a sudden claiming ownership for the software for one reason or another, I don't think that should be taken as a legitimate claim. From the moment one posts software on groupware or decides to data share, he or she looses sole possession of that software and cannot ever claim ownership of it!

T21 - Threat of compromising data integrity in shared databases by Simon Ruiz

1. What are the issues associated with this subject?

The issues associated with the sharing of databases are concerned with the administrators' decision granting level of accesses, limitations to users to whether they can delete/add/edit the data on the database(s). By that, it may or may not cause accidents to happen when users edit the same data at the same time. For example, if User A and User B wanted to fix the exact same data or the datum on the database(s) on a simultaneous timing, the computer can not distinguish which command to follow. This is presuming that the administrator gave access to the users to edit the data he or she has created.

2. How did this technology emerge?

The technology of sharing databases emerged from the need to share data to non-administrators such as customers and users who need the information of a particular group's data. The distribution can however vary, but the raw data can be shown through various ways, and on an important note, just the data.

3. Who are the stakeholders?

The stakeholders, the one actually holding the bet, will be directly the administrator(s) of the database(s) who will want reliability of the database to be valued high among the users.

4. What are the advantages and disadvantages for those stakeholders?

The advantages and disadvantages are hard to evaluate for the administrator(s). The one possible advantage for the administrator will be that he has all the power to change whatever he wants at the database and yet it can be a disadvantage too. For example, if he lets many users have access to the data to the level of adding/deleting/editing the data, it is possible that they could indicate errors within the database(s). On contrast, when many users have the right to edit data, again, the computer will be unable to distinguish which command is definite, causing a distortion within the database(s).

5. What solutions can overcome the problem?

Some of the basic solutions for this are the presence of passwords. Passwords will actually guide to the specific users to specific information and nothing more than that, which can be efficient if the password is not hacked, of course. Another solution will be for the administrator to limit the advantages of the user's level of access to the database in order not to cause the accidents within the database(s). Also, the administrator can create another database(s) exactly the same, in order to backup if the distortion happens caused by the users.

6. What areas of impact does it affect?

The areas of impact are directly concerned with the significance of the database(s). It will directly affect the knowledge of the user accessing the data from the database whether the data is accurate or inaccurate.

7. Evaluate the impact locally and globally.

To determine the impact of the database in local or global terms will again to evaluate the significance of the database(s). For example, if every information were deleted in "Google", a huge database, the whole world would probably start to panic and cause chaos. On the other hand, if a database is deleted for a unknown school in the jungle of Papua New Guinea, the impact would only affect the very few students and staffs involved to the school.

8. What are the ethical issues?

The ethical issues involved in sharing databases concerns netiquette. Netiquette is a word combined with the word "net" and "etiquette". If a generous administrator gives the user the privilege to change almost everything to a database, it is up to the user whether he will make good use of the privilege, or to vandalize the data stored inside the database(s). There are some cases such as hackers hacking inside restricted databases, for instance the database of the Pentagon. The hacker can say that he had the right to see the information because the information was there for him to see, regardless of how high the security was.

9. Who is responsible?

Ultimately, the responsibility will all be on the administrator(s) because they have the actual control whether to limit the privileges of the users. Whether they apply passwords or other restrictions, it is up to the administrations for the concern of the network security level which determines the reliability of the solutions.

10. Who is accountable?

Again, the important note is that the administrator(s) gets to ultimately decide the limitations of the users. Network security will be another task responsible for the administrators but if a distortion happens within a database, the users will have the privilege to distort it but not until they can fix it.

11. What laws apply?

At this moment, the laws that apply to sharing databases are limited among few authority figures that consider the database to be top secret or important not to be shared among common users. Laws concerning databases are not commonly known but as still considered as the basis of netiquette. The laws that illegalize the abuse of databases will soon be suggested.

12. Are there alternative decisions?

The alternative decisions for the sharing of databases would be simply just not create databases that can be shared among common users. That is the extreme case. Administrators often are innovative at the limitations that the users can have when they access the data on the database(s). Some examples include technology for what time the users can access the database, avoiding errors when the editing of the data is done simultaneously.

13. What are the consequences of these decisions?

The consequences of these decisions concern the rights for the users to access the level of information they can delete or the timing they can access. The objective of the database(s) is for merely for the administrator to provide the information to the specific users who value the information as a necessity. But again, the equity of sharing database(s) causes many distortions within the database.

T22 - Additional threats to privacy on a network compared with stand-alone computers by Tanay Khandelwal

A stand alone computer is a self-contained computer, usually a microcomputer, which is not connected to a network of computers and can be used in isolation from any other device.

The issues associated with stand alone computers are that stand alone computers require all the power from their own computer to conduct tasks and access the internet. This can be a major problem because sometimes a computer may overload or go beyond the limit of its CPU usage and crash. But, at the same while, stand-alone computers, though not the general systems used at all anymore, are highly more reliable than the computers we use in modern days which are hooked up to the internet. This is due to the fact that, stand-alone computers in general are not hacked into, and do not pick up viruses as they run as a self or “individual.”

Stand Alone computers run on an old modem internet connection of about 28.7 kbs. This way, downloads would take up to 60 to 70 days!

A “network computer” is a computer with minimal memory, disk storage and processor power designed to connect to a network, especially the Internet. The idea behind network computers is that many users who are connected to a network don't need all the computer power they get from a typical personal computer. Instead, they can rely on the power of the network servers.

Stand Alone computers today include: applications such as servers, games, and programs that have been made to “stand-alone” themselves.

Network computers are highly dangerous though a use of computer technologies today in order to be more efficient. Network computers are designed to minimize the amount of memory and processor power required by the workstation. Though to the average Joe, this may seem very advantageous it is rigged with problems. Network computers, if not protected with the correct virus-defense mechanisms, can be hacked easily and users’ information can be used in negative aspects. This is due to the fact that it is linked to a server which is shared. For example, just recently in the past year or two, CIT had an outbreak of a virus called “BugBear” that spread across the campus. This was due to the fact that, one computer which was linked to a network had received this virus. Then, many computers on that same network, started to receive the same virus due to the fact that they were sharing the very same network that the virus had infected. Through this example, it is clearly presented that network computers can be much of a threat to an individual using it.

Furthermore, network computers, proved inefficient since it requires a network connection to run. This is a disadvantage as many countries/ places lack network connections. Also, no privacy is really present in a network computer as it is not designed to protect others from accessing its database, but rater vice versa.

Network computers today include: Acorn computers, Gumstix' netstix computers, Applied Data Systems Single Board Computers, NetProducts NetStation, Sun Microsystems JavaStation, RCA Network Computer, IBM Network Station, Apple Interactive Television / Apple Set Top Box, Model M4120.

T23 - The need to authenticate information by Vaibhav Bhandari

What is authentication? And why is it so important?

In a world full of innovative ideas, authenticating information online is becoming necessary, as its presence prevents us from facing consequences that lead towards several ethical and social issues. Authentication is the act of establishing or confirming something. This is becoming a neccesity and is vitally important, as it provides a safe and trustable network. In more simpler words authentication is the process which enables to verify a digital identity of a sender. It is a key aspect of trust-based identity which provides a codified assurance of one user to an another user. A common example of this is a request to log in. This can be things such as credit card numbers, and passwords.

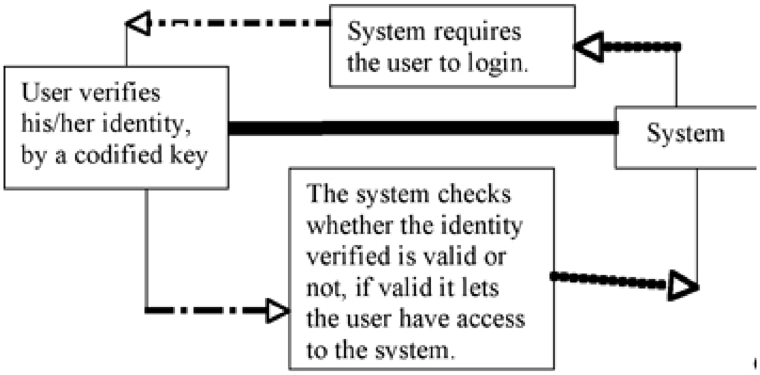
Places where information needs to be authenticated

- Accesing Email's
- Using an Internet Banking System
- Withdrawing cash from an ATM machine

*In all these places a login is needed, therefore inorder to login to the system it requires for the user to verify his identity by codified passwords.

What are the consequences if there is no authentication?

In simple words if there is no authentication it would enable anyone to access any indentity and manipulate or destroy data. More precisely it would become possible for anyone to login into any place, where in the presence of authentication it would require a user to verify his/her identity. This would mean that systems without the presence of authentication wouldn't require a login and anyone could log onto anywhere that they wish to login. Hence this brings up various consequnces which result into several social and ethical issues.


System requires the user to login.
User verifies his/her identity, by a codified key
System
The system checks whether the identity verified is valid or not, if valid it lets the user have access to the svstem.

Visual Demonstration

A demerit of Authentication – Phishing

One of the most major consequences faced because of authenticating information is as a result of phishing. Phishing is a criminal activity using fraud computer techniques (social engineering). The main objective of phishing is to fraudely acquire sensative information. Meaning to falsely acquire credit card numbers and passwords. This is usually done by sending a disguised email or a disguised announcement and asking the users to verify their identity. In this case they are not actually veryfying their identity but they are actually providing their sensative information to the phishers.
Major questions to be considere when writing the IB exam-

1. What is an alternative to authentication? Is it reliable? Is it secure?
2. What is a solution to the demerits of authentication? (What is a solution to phishing?)
3. What are the impacts of Authentication globally and locally? (What are the issues arised by phishing?)

T24 - Intellectual property protection on networks, for example, site licences, file access by Su Chen

Recently, people are intended to focus more on the intellectual property protection. Countries have comprehensive laws for the protection of intellectual property (IP), which conform to all the major international IP conventions. They are commensurate with its status as a developed economy. The framework is intended to encourage creativity and ensure that creators enjoy the results of their innovations.

In other words, Intellectual property refers to creations of people’s mind which include inventions, literary and artistic works, and symbols etc that designs used in commerce (in public). Later on Intellectual property divides into two categories as what we know: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indication of source; Copyright which includes literary and artistic works such as novels, poems and plays, films, musical works. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcaster in their radio and TV programs.

Thus, countries like Japan has the Intellectual property Department monitor the Intellectual property regime and ensure enforcement. It investigates complaints against infringements and has extensive powers of search and seizure. There are a lot of option affording protection, but depending on the item to be protected such as Patents, Trade marks, Copyright, Registered design.

Before, society only focuses on the basis of Intellectual property protection. They only care about the property that actually exists (physically), like trademarks, patents. However, in this fast growing society, network gets more and more important, little by little it involve in every activity. Thus, later on people Intellectual property add the network protection into its category, such as file access and site license which also involve in copyright. Finally, the Intellectual property protection changes some specific part in the protection list. They clam that Copyright is no longer only use for the book, photo these things. The filed copyright and relate rights has expanded dramatically as technology development have brought new ways of disseminating creations worldwide through such forms of communication as satellite broadcasting, compact discs, DVDs and the Internet.

Everyday, we will face the intellectual protection whether you are consciously or unconsciously. You may never know what site license is because without knowing it you still can use the internet. However it is very important since a site license allows you the right to copy a specific software product across multiple machines in your organization. Generally site licenses define an organization, location, or other means to describe the “site.” Although without the site license you can still download or copy from other computers in your local area network. In fact, at this time you already broke the law of Intellectual property protection. There is a very good example of site license: Adobe software (reader and flash player). Adobe Portable Document Format (PDF) lets you capture and view robust information — from any application, on any computer system — and share it with anyone around the world. The problem of PDF is that it captures or searches the information (document) freely without limitation.

Site license does not work in PDF which means in local area network, adobe can freely to download view robust information from any other computers that in the same local area network without site license. Although, some one may just argue that this is not a big deal, adobe is an efficient tool. In fact, there are some problems (debates) rises from this function. In one hand Adobe saves our time and makes our lives more convenient. But in other hand, it breaks the Intellectual property protection. The owner of some specific program (documents, software, music, etc) will lose their property since Adobe is freely downloaded from any other computers. It invades our privacy. Therefore the question is should we allow Adobe to do so?

The social and ethical issue of Intellectual property protection on network is that the owner of his/her property has the authority to choose whether wants to share on the network or not. Every other individual has no right to download or copy it from the network (especially for some bad purpose) without site license or owner’s permission. Privacy becomes a very important point. Without the protection, no one is going to share information. People will afraid that sometimes their personal information may just disseminate on the internet. Their work might be stolen by some people. Therefore in some senses, the Intellectual property protection provides a “safe” space that people can actually do some secret things. In the meantime,

Intellectual property protection not only provides the privacy of the information and inventions but also protect the accuracy of it. So, without owner’s permission, individual can not change the information or invention purposely. From the society point of view, it encourages people to invent new software and programs since creators can be given the right to prevent others from using their inventions, designs or other creations and to use that right to negotiate payment in return for others using them. For example, without protection your program can be patented. Someone can steal your program and change it and then share or sell on the internet. To be considered, governments and parliaments have given creators these rights as an incentive to produce ideas that will benefit the entire society.

T25 - Equality of access for different groups and individuals by Dhruv

A network is a system of computers interconnected by telephone wires or other means in order to share information. All the computers at, for example, a banking firm, may form a network. They all have information that can be input and read at any of the locations with adequate security clearances. Depending on the levels of clearance, a person has more freedom in a network. The internet is also a network.

1. What are the issues associated with this subject?

There is a certain inequality of access. Only the CEO would be able to view all available information. An accountant could only access transaction records and only the Admin people will have the power to modify the network. Another network privilege would be the Admin people's abilities to bypass filters that all other employees may be subject too. Everyone does not have equal access to the network. . On the other side, it is possible that control of access, if done fairly, may prevent people from meddling with the network. Censorship, is another issue in network equality. China censors many anti-government websites to control its people. This is inequality of access.

2. How did this technology emerge?

In September 1940 George Stibitz used a teletype machine to send instructions for a problem set from his Model K at Dartmouth College in New Hampshire to his Complex Number Calculator in New York and received results back by the same means. This was the precursor to all modern networks.

3. Who are the stakeholders?

The stakeholders are the people who's access is being restricted and centered and the people doing the 'restricting'. The restrictors believe that inequality of network access would have a positive impact for their countries or companies. In the case of countries, internet censorship is sometimes abused to maintain a Government's power such as North Korea. It's people can't see the outside world, they don't understand the faults of there own country.

4. What are the advantages and disadvantages for those stake holders?

Let's talk about companies. The disadvantage for employees is that they are disconnected from other parts of the company. However, the benefit for the company is that people know what the need to know. This leads to better security and efficiency.

However, for countries, restricting internet access allows them only to strengthen there power. It may be detrimental for the people and takes away there freedom. North Korea is a good example for this. Its people don't understand the flaws of their government cause they have never seen any other government. Maybe they deserve this opportunity to see what the world is like to make a better.

5. What solutions can overcome the problem?

The companies have got it right. They have found a good balance in there restrictions. Regarding North Korea however, the UN may have to put pressure on it to reduce censorship. There is no guarantee that this will work.

6. What areas of impact does it affect?

7. Evaluate the impact locally and globally

It effects the company's economic well-being, having control over what they view and when they view. It increases productivity. So long as they don't restrict to a level that frustrates employees completely, and achieve a balance, the company will run smoother and better than without network accessing.

From the point of view of countries, it affects world politics. Censorship In North Korea will leave the people close-minded and possibly supportive of a nuclear war if North Korea gets involved in one. Getting rid of censorship could change the attitudes of people in N.K.

8. What are the ethical issues?

9. Who is responsible?

10. Who is accountable?

The obvious ethical issue would be “is it right to restrict access of something to people?” The people applying restrictions would be responsible for it. Thinking deeper, it is possible that misbehavior by employees may have resulted in a company putting controls on its network access. Indirectly, it can be the people. In the case of NK, it is the government that is responsible. In the same way, the government or people may be held accountable for having unequal internet access.

11. What laws apply?

The laws differ from country to country. Companies are allowed to apply controls on the network access to there employees within the confines of the company network. As countries go, some countries make it illegal to censor websites while others allow it.

12. Are there alternative decisions?

A government could change its policy on censorship and allowing networks to discriminate based on rank. Any number of variations of the present state of affairs could occur.

13. What are the consequences of these decisions?

The consequence of these decisions could be more network freedom for the employees. This may come at the cost of less revenue for companies in light of security risks. People could view whatever they wanted to and disrupt the organization. Even, just casually surfing the net would affect the company’s efficiency. If NK changed its stance on censorship, the government would surely be in trouble when people saw what the outside world was like.

T26 - Ability to monitor users (surveillance); concerns of people regarding monitoring by Taro Kondo

Monitoring, which is an essential factor for efficiency through network, can take several forms. Before explaining the numerous types, it is important to note more specificlly the reason behind monitoring.

As the internet started getting widely used, the network became more and more complex, which caused malfunctions once in a while. This included system failure or decrease in speed of running computers. An event which relates to this occurred at the time when people around the world were expecting a millenium. When the timer changed to year 2000, some of the transimissions of data went to wrong directions and a temporary disorder spread. Another case which was rather common, (still happening today) was when numbers of users accessed to the same site, and consequently there was a 'traffic' within the network. This slowed down the transimmisions. In more worse events, there were 'overloads' and servers crashed. That explains why sometimes when you go to certain websites, a page with a white background stating 'access denied' or 'connection cannot be established' pops up.

In order to solve these matters, an idea of 'network monitoring' arose. The concept was that periodically, the monitoring system checks the network and if there is anything wierd going on, it informs the network administrator by either sending an email or some other alarm messege to him/her.

Besides these issues however, other applications of monitoring should be taken into account. The terminology is 'intrusion detection system' (IDS) and what this does is also monitoring, but concentrating more on outside threats to the network. The system activates at times when there are attacks that cannot be blocked by firewall, such as manipulations to computer systems by hackers or automated tools through unauthorized access. The attackers might target vulnerable services and steal private information, set viruses, etc.

For monitoring these kinds of situations, the system used is more complicated than the system for preventing traffics. It has three major components, which are sensors, console and engine. Sensors create security events, console monitors the events, and engine keeps track of the events. The reactive state of IDS due to attacks, is resetting connections and reprogramming the firewall. In addition, it alerts the operators. If the attacks are not apparent and there are just 'holes' in the security, the system records them and sends alerts.

Monitoring without the use of systems is not rare. For example in Limewire, which is a peer-to-peer file sharing program, occasionally members of the police do what is called a 'net-patrol' and they search for any malicious files that are uploaded. These may be files which have spywares attached to them. Not only those, the police look for files which disregard copyrights, such as music created by famous artists or televised movies. The sharing of such files is one of the greatest problems occuring today through the network.

The ethical issue relating to monitoring as a whole, is that people are concerned about their privacy. Especially in the case of manually operated monitoring, the people who monitor are able to see exactly who is sending or receiving what, even the things they are not intending to investigate. So these days under certain laws, the users are set to anonymity, unless they do something bad. Again Limewire as an example, if the police notices an infringement, he contacts most likely the programmer of Limewire to track down the person who violated. Although anonymous, the users will be distinguished somehow, probably by IP, so that in this sort of situation they can be identified. In the entire network, this measure is commonly practiced.

T27 - Ability to filter incoming data by Alex Young

With the internet being a major part of our everyday lives, one must get to know more about network filtering. Network filtering is used by blocking incoming information or placing certain information through a certain network filter. For example, in Yahoo! e-mail accounts, there are filters for suspicious mail (such as a virus or spam) and places those mails automatically to the bulk folder which separates it from the inbox folder. Also there are certain software that filters certain websites such as St. Bernard or even antivirus programs such as McAffe software which restricts certain websites by the content they include (Such as spyware/adware adult content, shareware, gambling).

In today’s world the Chinese government has a major filtering program, which restricts certain images in search engines such as Tiananmen Square which shows peaceful images in Google China while in Google US, it shows the tanks on the streets of the infamous day. Also, Google China censors certain search terms from showing up such as (adult content) or content in which the Chinese government feels vulnerable to its own country or makes the government look bad.

4. What are the advantages and the disadvantages for those stakeholders?

Web filtering can be an advantage if the Chinese government is censoring certain images and websites because they don’t want certain people accessing them such as a gambling site. The disadvantage is with the web censoring in China through filtering, is it causes controversy as to whether or not this is an human rights violation because it restricts Chinese citizens because the government of China redeems as harmful for the country. What if in fact is not harmful for the country but in fact the Chinese government is filtering certain websites because they don’t want the Chinese people from knowing the truth or make the Chinese nation look bad (Tiananmen Square).

5. What solutions can overcome this problem?

One way for the Chinese people to try and go around the filter is to try to hide the internet’s IP address. An IP address is the numeric address of a computer connected to the internet. This can locate what country he is using the internet and also approximately identify where in the country he lives. Therefore each country has certain numbers assigned to know what country it is coming from and the other numbers further identify and separate from one user of the internet from another. There are software in the world to try and hide or conceal the computer’s IP address to not be identified. This can be useful for people because if people are downloading from torrents, the government cannot find out where the person is downloading from. Also in the case of the Chinese people, they can now access certain sites. Another option is to use a different IP address to try to also hide the real address (which is your computer’s network). Although these alternatives are nice, they often do not work well because it is hard to find software to try to conceal the IP address. Also, with the option of trying to use a different IP address it is not reliable as most of the ones shown on the internet do not work and even when they work, they are very slow.

6. What areas of impact does it affect?

Obviously, with network filtering, it affects to whoever is using the internet and where they are using it. Fortunately in the US, they do not follow the Chinese filtering doctrine and instead lets the people live in America surf whatever they want.

8. What are the ethical issues?

Although filtering certain junk mail to the bulk folder or using anti-virus programs or software to filter us from entering websites we have no intention of going to is useful, the Chinese government’s strategy of censoring certain websites is ethically wrong because it deprives the Chinese people from entering certain web sites because of the filtering and therefore is taking away the basic human right for Chinese citizens which is to freely surf the web.

T28 - Ability to control personal, business, military, government operations over a wide geographical area by Ronald Chu

There are several ways to control personal, business, military, and government operations over a wide area. However, what are these four things? These four complex operations are what make up our daily lives; they may seem simple and easy but they actually consist of small groups of similar operations. The main thing that is contributing to the control of these operations is the establishment of our technology, which is improving daily.

First of all, what are personal operations? A personal operation is something such as a personal phone (cell-phone) or PCs (personal computers). These kinds of extremely convenient systems allow you to keep in contact with others as well as giving you different forms of information and entertainment. There many different companies and organizations producing and providing us with these systems. Take DoCoMo (cell phone) for example. They sell us cell phones as a product, and the way we use it is completely up to us. However, they "control" it in a sense that they make us pay monthly bills and can even keep track of everything that we do with our phone (how we use it). The main social questions concerning this issue are how this technology emerged and what areas of impact it affects globally and locally. The main ethical questions are if there are any alternative decisions (such as switching telephone companies or even to other means of communication) and what the consequences to these decisions are.

Secondly, what are business operations? According to an online definition from www.wikipedia.org, business operations are those activities involved in the running of a business for the purpose of producing value for the stakeholders. The three main objectives of a business operation are to 1: generate recurring income, 2: increase the value of the business it is doing, and 3: secure the income and value of the business. Toyota Motor Cooperation is the eighth largest company in the world, as well as a very well known and successful business operation. It makes thousands of cars per year (not including any other of its many products), has stores all over the world, and income pouring in. How do they even control all of this? Ability to control/stabilize depends on how well a company can "protect" its income from generating capability and retains its value as a business operation. The main social questions concerning this issue are who the stakeholders are, what their disadvantages and advantages are, and what areas of impact does it affect globally and locally. The ethical questions are the same as personal operations.

Third of all, what are military operations? A military operation is the employment of military resources to achieve a certain goal. It involves the planning, calculating, or the giving (or receiving) of information. There are military operations other than those concerning war. For example, the US has military operations focusing on promoting peace and supporting civil authorities in response to any disruptions within the country. There are several ways the military controls these sorts of operations. They can use satellites to "keep an eye" on everything going on in the world. The main thing that helps is the fact that one man has total control over everything to do with this subject. If there were many leaders, then there would be confusion, but since there is only one military commander, he makes all the decisions and there is total command. The main social question concerning this issue is what areas of impact it affects locally and globally. The main ethical questions are who is responsible and accountable, and what laws apply.

Finally, what are government operations? Government operations are anything to do that the government has been involved in, such as good (coal, oil, steel, etc) and service (insurance, law, police, etc) operations. The government can sometimes have certain control over business operations. Government operations are not usually controlled, but they are the ones that control us. However, they can be controlled in a sense that without our taxes, they do not have power and also, we elect who is our leaders are. The main social questions concerning this issue are who the stakeholders are, and what areas of impact it affects locally and globally. The ethical questions are who is responsible and accountable, what laws apply, and are there alternative decisions (such as anarchy, or a dictatorship) and what the consequences to these decisions are.

T29 - Increased globalization, for example, EFT, EDI, e-commerce by Aditya Kumar

Electronic commerce (also referred to as EC, e-commerce or ecommerce) consists primarily of the distributing, buying, selling, marketing, and servicing of products or services over electronic systems such as the Internet and other computer networks. It can involve online marketing, supply and also electronic funs transfer (EFT), inventory management systems; automated data collection systems and electronic data interchange (EDI). As per Forrester Research, electronic commerce generated sales worth US $12.2 billion in 2003.1

General Pros

Electronic data exchange eliminates costs that are usually incurred as a result of publishing, printing or producing hard copies of something. This is can promote unethical behaviour in that it is simpler to engage in piracy with electronic information rather than hard copies. This is because it is difficult without fairly sophisticated equipment and expensive software to 'electronify' data from hard copies. Another benefit of globalization in the form of electronic data transfer is efficiency as a result of minimal time wasted. Through quick processors, data can be transferred quickly and also no time is wasted in printing information. Another way that this technology can save time is because one has the power to track the origin of the information which they are receiving thereby reducing time spent corresponding with the sender of the information.

Stakeholders

Companies also adopt this technology as a means to save money. For example, a company probably will save money in the long run by saving on publishing, shipping, and handling costs. Two parties can communicate with each other quickly, being efficient, and also clarify information that they receive to be true. Another reason why companies might embrace this technology is because it might aid in the sales of their products. A customer needn't go through the hassle of going to a shop. He is satisfied just sitting at his computer and making his purchase. Firewalls and encryption tools make electronic transfer of information reliable and secure. It is a smart way to keep customers satisfied and hungry for more.

Instance of problems with technology

According to Wikipedia, the set up of networks to engage in the electronic transfer of information can work out to be quite expensive. Also, another disadvantage is that the high speed of electronic data interchange can result in the reception of an invoice before the actual reception of a good. This might work out to be cheating someone else because one is forced to pay for something he is not yet sure he has received.

Ethical problems

E-commerce could also be through the form of advertising a product on the web. A flaw with this is that anyone can post any information on the web and can misinform people about a product. This is unethical in that a consumer can be conned into buying the product which is not truly what it claims to be. By doing this, one stems the sales and channels business to itself. Also unfair is that data can be manipulated by anyone who can manage to hack into a server. Also, is the question of funds exchange over the internet. Many times, companies like E-bay, which co-ordinate the selling of goods by one person to another, refuse to take responsibility for sellers who con people. Sometimes packages are delivered without any contents.

Also, the refusal to take responsibility allows for people to cheat one another often and without difficulty. Another flaw with this is that people are required to pay for a good with their credit card before actually receiving the shipment and checking to see the contents of the package being shipped to you. Since it is easy to change information on web pages, someone with access can very easily modify electronic data without being tracked. Also done by some is to fraud others by finding a credit card number, lying that it's secure and using that number to buy products from somewhere else. This is of-course not done by reputed companies.

Some people might not be able to fight the urge to intercept data and use it to their advantage. A way to combat this might be encryption but in a rivalry between two large companies such as Apple and Microsoft, both probably have encryption battling algorithms in their arsenal allowing for one to profit from the other's innovations. So essentially, globalization in the form of electronic commerce has both its pros and cons when it comes to ethics.

T30 - Need for interface standards by Dwarkesh Iyengar

What is the Technology?

In telecommunications, an interface standard is a standard that describes one or more functional characteristics (such as code conversion, line assignments, or protocol compliance) or physical characteristics (such as electrical, mechanical, or optical characteristics) necessary to allow the exchange of information between two or more (usually different) systems or pieces of equipment. An interface standard may include operational characteristics and acceptable levels of performance.

What are the issues associated with this subject?

User interface standards have become the object of increasingly intense activities in recent years including work in the International Standards Organization (ISO) and the European Community. These activities are part of a general concern in information processing standards but are also based on the widely held feeling that consistency is one of the most important usability considerations. Even though consistency is obviously not the only usability factor, there are still good reasons to obtain it in balance with other usability considerations in a usability engineering process, and such additional considerations are indeed also included in many current standards activities.

Who are the stakeholders?

The responsible developers have different perspective about the problem. Based on a report conducted by the ISO- The products of developers and companies deviated from the standard due to the fact that the developers mostly claimed that they had chosen alternative design solutions because they had found them to be better than the one mandated by the standard. Other explanations were that the development tools did not allow compliance with the standard and that the developers had indeed planned compliance but had not yet had time to implement it. Further explanations were that the developers were not aware of the rule they had broken or that they had overlooked the deviation. In no case did it turn out that the developers had actively misinterpreted the standard and designed a specific deviating interface feature in the explicit belief that they were following a rule from the standard. This indicates that the individual parts of the standard are reasonably understandable - perhaps because the standard almost always contains elaborations of the rules and backs them up with a rationale.

What are the advantages and disadvantages for those stake holders?

Benefit for users:

- Flexible systems built from interoperable components.
- Multi-provider solutions reduce lock-in.
- Maximal utility, minimal cost.
- Benefits for providers, developers, vendors
- Opens up a healthy component marketplace.
- Conformant software is more marketable.
- Easier to specialize in one field or component (don't have to provide a complete or general solution).

What solutions can overcome the problem?

To increase the usability of user interface standards, some steps could be taken by having development tools or Web templates that support implementation of interfaces that follow the standard including many concrete examples of correctly designed interfaces making sure that all examples are 100% compliant with the standard complying with older standards as much as possible.

What areas of impact does it affect?

The deviation from the standards affects the quality of the interface and thus results in an impact on the people and their usage standards. This results in them turning to other available options and thus negatively affecting the developer or the company.

T31 - Need for network use policy by Marek Strzepek

To fully understand the concept of networking, it would most probably be useful to study the definition of it. In the Encyclopedia Britannica, it is defined as “The scientific and engineering discipline concerned with communication between computer systems. Such networks involve at least two devices capable of being networked with at least one usually being a computer.”

These days, many corporations have integrated their computer together to form a much faster, efficient machine to process all the data. By connecting all of their computer drives together, the information can be much more easily accessed and valuable time saved. This function is especially useful for large companies which have numerous customers and several deadlines to meet. Networking is known to be a process that maximizes the amount of production without purchasing addition machines. It is also extremely cheap to implement and can substantially increase a company's production in a very short period of time. An apt description of this networking could be said as “The whole is more valuable than the sum of its parts”.

However, this efficiency does not come without its price. By linking all of the computers together, not only can information spread faster, but viruses as well. If one act of careless occurs and a single networked computer is infected by a virus, the entire system could be bought to its knees. This reason alone has been why some of the more cautious companies have refused the offer to “chain” their computers together.

The history of networking is a long and illustrious one, beginning with the linking of two computers from Dartmouth to New York. The individual that accomplished this magnanimous action was none other than George Stibitz himself, who did this in order to send his complex mathematical equations to himself via a teletype machine. This is the earliest recorded example of computer networking occurring and is assumed to be the first time it ever happened. However, there are claims that during the exact same year, the M.I.T. (Michigan Institute of Technology) and launched and succeeded in their first test of computer networking. Therefore, the issue of who actually first completed a computer network is still in dispute. But, one fact that is for certain, is that by the 1970's, almost all of the major universities in the United States were utilizing computer networks to further enhance their academic efficiency.

The most commonly known factor of computer networking would have to Local Area Network, which is more commonly known as LAN. This allows individuals in close proximity to each other to trade information and other essentials via computer files. It is also the technological marvel that allows the average teenager to play computer games online at his friend's house, should he bring his laptop over there.

Recently, WLAN has appeared all over the web. The W stands for Wireless, and it is fast becoming the most popular way of trading information in a local area. The reason for this is self-explanatory, mainly because there are no wires. This allows increased mobility for all computers (mostly laptops) and allows for less risk for accidents, as there are no wires to trip over/get tangled. Therefore, this has become an extremely positive advance in modern society.

All in all, the integratation of computer networking in today's society is vital, as it helps a multitude of things in order. It has helped students complete their homework, kept companies running, and informed Interpol of the whereabouts of several suspected criminals. Its functions are as numerous as they are useful, and today's society would be struck a terrible blow if we lost this network for a single day. It is the epitome of efficiency in current civilization and we all would be lost without it.

Knowledge of technology

In order to study and evaluate the social and ethical issues involved in the use of networks the student must have an understanding of related technological concepts. These may include:

T32 Key Terms by Chirag Garg

LAN, WAN, client, server, Ethernet, access, access permissions, login, password, firewall, sysadmin, UPS, EDI

LAN

It is a computer network covering a local area, like a home, office, or group of buildings. Current LANs are most likely to be based on switched IEEE 802.3 Ethernet running at 10, 100 or 1,000 Mbit/s or on Wi-Fi technology. The defining characteristics of LANs in contrast to WANs (wide area networks) are: their much higher data rates; smaller geographic range; and they do not require leased telecommunication lines. Thus, some of the issues with LAN are that they have a small geographic range, and as there are numerous systems connected to one, there are more chances of getting them infected my viruses and hackers etc.

WAN

A Wide Area Network is a computer network covering a broad geographical area. Contrast with personal area networks (PANs), local area networks (LANs) or metropolitan area networks (MANs) that are usually limited to a room, building or campus respectively. The largest and most well-known example of a WAN is the Internet. WANs are used to connect local area networks (LANs) together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. The different types of WAN's are Leased Line, Circuit switching, Packet switching, and Cell relay. These different types of WAN's have problems like call setup, expenses, fixed amount of the transfer of data etc.

Client

A client is a computer system that accesses a (remote) service on another computer by some kind of network. The term was first applied to devices that were not capable of running their own stand-alone programs, but could interact with remote computers via a network. These dumb terminals were clients of the time-sharing mainframe computer.

The client-server model is still used today on the Internet, where a user may connect to a service operating on a remote system through the internet protocol suite. Web browsers are clients that connect to web servers and retrieve web pages for display. Most people use e-mail clients to retrieve their e-mail from their internet service provider's mail storage servers. There are basically three types of clients, the Fat Client, the Thin Client and the hybrid Client. Thus, the fat client gives a high performance and support but have low manageability and flexibility. The thin clients give high manageability and flexibility but don't have a high performance and support.

The hybrid clients have all the above features of the fat and the thin clients.

Server

In information technology, a server is a computer system that provides services to other computing systems—called clients—over a network. The term server can refer to hardware (such as a Sun computer system) or software (such as an RDBMS server). Although servers can be built from commodity computer components—particularly for low-load and/or non-critical applications—dedicated, high-load, mission-critical servers use specialized hardware that is optimized for the needs of servers. For example, servers may incorporate "industrial-strength" mechanical components such as disk drives and fans that provide very high reliability and performance at a correspondingly high price.

Ethernet

Ethernet is a large and diverse family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, two means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format. Despite the huge changes in Ethernet from a thick coaxial cable bus running at 10 Mbit/s to point-to-point links running at 1 Gbit/s and beyond, all generations of Ethernet (excluding very early experimental versions) share the same frame formats (and hence the same interface for higher layers) and can be readily (and in most cases cheaply) interconnected. Due to the ubiquity of Ethernet, the ever-decreasing cost of the hardware needed to support it and the reduced panel space needed by twisted pair Ethernet, most manufacturers now build the functionality of an Ethernet card directly into PC motherboards, removing the need for installation of a separate network card.

Login & Password

A login is the process of receiving access to a computer system by identification of the user in order to obtain credentials to permit access. It is an integral part of computer security procedure. A username is used in preference to the full name of the user this is a shorter sequence of characters which still uniquely identifies the person. A password is another sequence of characters which provides the user with a key to the system and is kept secret from others. The issues with logins and passwords are that there is a chance of other people trying to get the login and passwords and misuse it. Thus, people usually keep the passwords complicated or personal due to which they are hard to remember and which is why people have a chance of loosing them.

Types of Intrusion

Different types of intrusions are like Viruses, hacking etc. A computer virus is a self-replicating computer program written to alter the way a computer operates, without the permission or knowledge of the user. Though the term is commonly used to refer to a range of malware, a true virus must replicate itself, and must execute itself. The latter criteria are often met by a virus which replaces existing executable files with a virus-infected copy. While viruses can be intentionally destructive—destroying data, for example—some viruses are benign or merely annoying. A hacker is someone who creates and modifies computer software and computer hardware, including computer programming, administration, and security-related items. The term usually bears strong connotations, but may be either favorable or denigrating depending on cultural context.

T33 - Security Measures by Wilanth James

What is computer security? Computer security is the process of preventing and detecting the unauthorized use of one’s computer. To stop unauthorized users (known as “intruders”) from having access to any part of one’s computer system, there are prevention measures one can use. Also, detection helps to determine whether or not someone attempted to break into one’s system, and if they were successful, what they may have done.

In recent years, many households use computers for everything from banking and investing to shopping and communications with others through e-mails and chat programs. Although many people might not consider their communications “top secret”, no one would want ‘intruders’, from reading their e-mail, using their computer to attack other systems, sending forged e-mails from their computers nor personal information stored in their computer (such as financial statements) examined.

Intruders (also known as hackers, attackers or crackers) may not care about a person’s identity. Whenever they are bored (also maybe if their life has no bright side to it), they would hack into a computer to gain control of one’s computer so they can use it to launch attacks on other computer systems. By doing so, they avoid being traced directly to their computer system at they break into high-profile computer systems such as government or financial systems. Even if the computer in the particular household is used to play the latest games or to send e-mail to friends and family, that computer maybe targeted. Intruders may be able to watch all the actions of that household computer or cause damages to it by reformatting the hard drive or changing data.

Unfortunately, intruders are always discovering new vulnerabilities (informally called “holes”) to exploit in computer software. Software complexity makes it increasingly difficult to thoroughly test the security of computer systems. When holes are discovered, it is up to the user of the computer to obtain and install the patches to address the problem or correctly configure the software to operate more securely. If system administrators and users kept their computers updated with patches and security fixes, most of the incident reports of computer break-ins could have been prevented. Also, some software applications have default setting that allow other users to access the computer unless the user changes the settings to be more secure. An example includes chat programs that let outsiders execute commands on one’s computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them.

A firewall is a system or group of systems that enforces an access control policy between two networks. A firewall typically takes one of two forms in the context of home networks. One is in the form of software firewall which is a specialized software running on an individual computer. The other is a network firewall which is a dedicated device designed to protect one or more computers. Many of both types of firewalls allow the user to define access policies for inbound connections to the computers they are protecting and also provides the ability to control what services (also known as ports) the protected computers are able to access on the Internet (outbound access).

A variety of antivirus software packages that operate in many different ways, depending on how the vendor chose to implement their software. But they all look for patterns in the files or memory of your computer that indicate the possible presence of a known virus. Antivirus packages know what to look for through the use of virus profiles (sometimes called “signatures”) provided by the vendor. Since new viruses are discovered daily the effectiveness of antivirus software is dependent on having the latest virus profiles installed on the computer so that it can look for recently discovered viruses. It is important to keep these profiles updated.

T34 - Network types, for example, Intranet, Internet, VPN by Oliver Chan

Internet

The internet is the type of network that’s most commonly known. The internet is a worldwide network that is constantly growing, sometimes described as a “network of networks.” The internet uses a common protocol (an agreed method of communication) known as Transmission Control Protocol/Internet Protocol, or more commonly know as its abbreviation: TCP/IP. The internet is an endless resource for information, where the word endless does not really emphasize the size of the network.

Intranet

An intranet is the internal network of an organization, such as company or school. An intranet uses the same network protocols and technology of the internet, but the access is restricted to employees, teachers, etc. It is sometimes described as the “private version of the internet.” An intranet is used to share information within an organization, and generally features a web server providing such information on the network.

Local Area Network (LAN)

Local Area Networks and intranets are quite similar in the fact that they are restricted networks. Most Local Area Networks tend to use the TCP/IP protocols, and most of them are connected to the Internet, commonly through a firewall. However the difference between an Intranet and a Local Area Network is that they don’t have a web server providing resource to the network.

Extranet

An extranet is two or more computers or a local area network connected via the internet. It can be described as a private internet over the internet. Extranets are sometimes used to extend the intranet to other users.

Wide Area Network (WAN)

A WAN is a network of two computers (or local area networks) that are connected over a large geographic distance through a dedicated connection. WANs are generally more expensive as they require the dedicated connection (not the internet), that is usually leased.

Virtual Private Network (VPN)

A virtual private network is two or more computers connected to each other via the internet. What separates the VPN from the other networks is its encryption. VPN generally involve high encryption in their data transfer as their medium for transmission is via the internet. Virtual Private Networks are generally favored over Wide Area Networks for their cost, as leasing a dedicated connection is more expensive than simply using the internet.

The ITGS viewpoint of networks

All the networks were derived from the network ARPANET, Advanced Research Project Agency network that was designed by the United States Department of Defense.

Everyone who uses the internet or an intranet is a stakeholder, and since networks are so commonly used, it hits almost all areas of impact. The issues arise when people try to ‘attack’ your computer and stealing personal information from it. When people try to hack VPNs and other private networks and steal information that can damage companies and corporations. Although our networks provide the advantage of ease for communication and sharing information and resources, the disadvantage of the risk of a security breach is definitely apparent. Since networks are used both locally and globally, the social and ethical issues apply on both a local and global level.

The solution, however temporary, is to fix the flaws of our networks: imposing more security and encryption in our data transfer, using firewall to make it harder for 'hackers' to intrude. This solution is temporary, as every network will have a security hole that's waiting to be found and to be exploited by hackers.

Ethical issues concern those who actually attempt at breaching the networks. The 'hackers' are both responsible and accountable, and the consequences of their actions are that they can be subject to be punished by federal law for intruding on the privacy of others.

T35 - Encryption and SSL by Nitish Gautam

SSL (Secure Sockets Layer) is a cryptographic protocol and applies cryptographic methods for such services like web email, web browsing, Internet faxing, etc. It provides authentication and privacy over the Internet using cryptography. SSL runs under protocols like HTTP, FTP, SMTP, etc. It also runs under various other applications, which form the TCP/IP protocol suite.

Encryption is the process of obscuring or hiding information so it is not read without any special knowledge. An example can be emails, and how passwords can be considered as special knowledge.

SSL was developed by Netscape and was released in 1996. Therefore, Netscape takes all responsibility for releasing it and developing it. And later, it served as a basis for TLS (Transport Layer security), later to be used by financial institutions like Visa, Master Card, etc. SSL had a big impact on the Internet. People started encrypting web pages, thereby making web pages hard to 'attack' and take over, as compared to earlier days, where there was no encryption and only normal encrypting methods were used.

It affected financial institutions the most, as they started using SSL on their home pages where people would log in and view their bank accounts on line. This was a big boom, and it provided safety for the company's website too. Also, before, companies would get attacked and they couldn't go anything about it. But now, their web pages were protected, and were secure. It had an effect on everybody, even on normal people who aspired to open websites and have SSL on them.

Some early weak points of SSL were that SSL could use only 40 Bit keys, because of legal restrictions. This was made so that they could read encrypted traffic. The US government explicitly imposed a 40-bit key space small enough to be broken by law enforcement agencies-wishing to read the encrypted traffic, while sting ll presenting obstacles to less-well-funded attackers.

There was also a time when the government wanted to encrypt emails and other forms of communication with their own encryption method. This was called (clipper?). This encrypted all emails, so that only the intended user can see them. But the government claims that it would have the encryption/decryption keys. This would result in our loss of privacy, and the government reading our stuff.

As SSL was introduced, people started using it incorrectly. Some websites only used SSL on the form submission page, but not securing the login page. This is hazardous, and SSL is not being used correctly, and also it is exposed to other people and can result in tampering and loss of information.

Basically, SSL is directly related to privacy. Companies used SSL to respect privacy and to ensure privacy. Now that web pages were more secure, users felt more secure, and started using the Internet more, as it became a safer zone.
And another form of insecure SSL is when it is not fully used. Sometimes, a website used SSL and other media and scripts along with it. This can also result in illegal results and furthermore, lower the safety of the website. The website is exposed more and can be attacked.

The advantages of SSL are that it secures the web page. It is also easy to use. It provides security more than any other protocol and it is used widely. Also, it cannot be broken easily, and prevents many attacks, including -man in the middle- attacks and so on. Also the data which is put in is processed with a different hash each time.

Along with advantages, are disadvantages. SSL can be broken into, it is not full proof. Also, many websites who use SSL tend to include other media and tamper with it, thereby making it insecure. Another disadvantage is that the certificates can expire, resulting in the same situation as without the SSL. Also, it is server dependent. This means that if a person gets into the server, then the SSL has no meaning. Another one is that it is used for only ONE page/email. This has limitations.

The advantage for Netscape is that it gets widespread publicity. SSL is used widely and they are also getting paid for it. This helps them and provides a cause. Also, another advantage can be that they are getting recognized. But also, SSL is like a open-source project now.

People have made many different forms of SSL using their source code, and added their name onto it. As we can see on the Internet, there are many free open source SSL projects out there. This is a disadvantage to Netscape, as their project is being literally 'plagiarized' by other people, or little companies.

Also, another point concerning encryption is a cipher. A cipher is basically an algorithm which encrypts. The cipher depends on a key. A key must be selected to encrypt a packet. Some types of ciphers include classical ciphers, polyalphabetic substitution ciphers, etc. Modern encryptions methods include symmetric key algorithms and asymmetric key algorithms.

Points to consider:
- Although SSL is encrypting information, it is creating a major gateway bottleneck. As secure sessions become more common, the gateway architecture is becoming less suitable for the servers.

- With encryption, there is a lot of server load since it encrypts each packet of information.

- It has a lot of cost for the systems handling encryption.

- Legal restrictions apply, as a company or the government cannot encrypt too much of a packet. A firm cannot encrypt more than a certain bit of information.

- During encryption, there are a lot of system crashes. And systems do not keep ‘backup keys’. The data, therefore, cannot be recoverable.

T36 - E-commerce by Harsh Sharma

What is E-commerce?

The “E” in E-commerce refers to electronic and therefore the term “E-commerce” means the buying and selling of objects electronically. It doesn’t only refer to buying and selling but also any other transactions over the internet for example electronic transfers of funds or money, online marketing and advertising etc. So a simple definition for E-commerce could be, “any transaction that uses the Internet.”

How did it develop?

It was first used in the 1970s when electronic funds transfer started to occur. And then in the 1980s, ATMs started to pop-up all over the streets and this caused an increase usage of the term “e-commerce.” And when the Internet came, it included online shopping and any payments made through credit cards. However, today it just doesn’t include online shopping and credit card payments, it also includes any kind of banking (funds transfer) or any kind of business related things taking place on the Internet.

Advantages and Disadvantages

Advantages:

1. Provides an easy and secure way for customers to purchase objects from their home. People don’t have to go to their nearest Wal-Mart anymore to purchase their favorite cologne. Everything is available on the Internet. You can make your purchase at any time of the day – 24/7! And as long as you have the Internet, you have access to all the products (even the products on the other side of the world).

2. There is no menu or catalog on Internet. Well there is some sort of index but unlike traditional menus, these indexes are updated hourly with new prices and new content – making it much easier for customers to select the right product!

3. There are less marketing expenses to be paid on the Internet. Cost of production is greatly reduced because there’s less labor costs and other processing (phone, fax) costs. Hence, that money can be spent on improving the quality of the product etc.

4. Everything is sold directly to the customers. There is no “salesman” anymore and that’s another reduced cost. It also builds the consumer-company relationship and solidifies it.

As stated before, e-commerce just doesn’t include the transactions of purchasing products online. It is basically any business related transaction done over the Internet. Therefore, there are other advantages that are not related to online shopping.

1. Employee can be trained on the web now. They don’t have to come to a specific place to be trained and that saves a lot of money. Employee can go on the Internet and learn from the updated material at their convenience.

2. E-mail has greatly reduced the costs of communicating between businesses and customers. Therefore, the prices of products on the Internet are cheaper than the prices in the real world because all these costs have been reduced!

3. Business partners can collaborate and work on the same project using many advanced programs available on the Internet and share their ideas without having to attend a meeting in Shanghai.

4. Instant updating is one of the main features of E-commerce. As long as you have the right device(s), instant updating of anything that has happened at the store can be done. So for example, an Apple store in Japan can update the recent purchase of a Macbook and the main Apple store in USA would receive that update in less than an hour and their accountants will be notified.

Everything has two sides. There are advantages and disadvantages for everything and E-commerce is not different. However, it can be easily deduced that there are a lot more advantages than drawbacks because of the wide-spread popularity of E-commerce.

Disadvantages:

1. Credit card transactions can be a problem for some (including my dad). Some adults think that their credit card number will be “misused” if they give it out to the Internet companies. They don’t understand how secure the system is but credit card frauds do happen and therefore these adults will never purchase anything with their credit card.

2. Some consumers consider shopping a “social event” as in they are used to shopping for hours with their friends and family and would rather keep it that way instead of spending 20 minutes on the Internet alone.

3. Some consumers want to experience and test the objects they purchase. Therefore, an object like a deluxe bed would be less sold than let’s say a computer software.

4. Time for delivery of the products can be annoying for some people especially if the shipping is done internationally! And it’s not just the time, there’s also a bit of uncertainty involved. When you do normal shopping, you walk out the store with your product in your hands but through E-commerce, the product will take time to arrive and even if the company sends it, there is not a 100% chance that it will arrive!

5. Returning goods can be a pain through E-commerce. You don't even know where your product came from then how would you ever return it?

6. Perishable goods cannot be bought over the Internet. Even though the companies are working their way around this by introducing advanced shipping methods, people still don’t trust them.

Again, E-commerce just doesn’t include online shopping and hence there are disadvantages including the other aspects of E-commerce too.

1. Hacking of an electronic system can easily be done in today’s world and therefore, any kind of electronic data is always at risk. The risk can be minimized but it will always be there.

2. Perhaps, the online interaction between businesses will not be good enough to finalize a deal because the business owner could feel like he doesn’t yet know the person because of minimal eye-contact required.

3. Computers are not perfect. With computers, anything can go wrong at any time and nobody can stop. The risk of that is being minimized everyday but it will never completely go away.

However, the advantages totally overcome the disadvantages and thus E-commerce is a very efficient way of doing business and therefore most companies today have websites and web stores!

The social issue related to this could be the fact that everything is going online and even less and less interaction between people is required. If this keeps going on, all of us will mainly be computers talking to other computers and there wouldn’t be any conferences or dinners anymore!

The ethical issue is of course the fraud and hacking involved. Credit card frauds happen all the time and that is the same as stealing.