APPENDIXES
NISER'S LINE OF REPORTING

Prime Minister

Prime Minister's Department

Chief Secretary

National Security Council

Ministry of Energy, Communication and Multimedia

MIMOS

NISER

Matters regarding budget, administration

Matters regarding security policy
ROYAL MALAYSIAN POLICE ORGANIZATION CHART (focus on department that investigate information warfare attack)

- Internal Affair Ministry
  - Inspector General
  - Deputy Inspector General
    - Management
    - Special Branch
    - Crime Investigation Dpt.
    - KDN/KA
    - Logistic
    - Narcotic
      - Forensic Lab
        - Physical
          - Computer Crime
        - Biology
        - Narcotic
        - Chemical
        - Mgmt.
          - Personal Computer Unit
          - Internet Unit
          - Software R&D Unit
          - Investigation Unit
        - Commercial Crime Investigation Division
          - Intelligence Unit
          - Technology Crime Investigation Unit
TRANSCRIPT OF INTERVIEW WITH AHMAD ZAKHI, DEPUTY PUBLIC PROSECUTOR ON 19 SEPTEMBER 2002

What is the major problem that makes computer crime offences do not end up with prosecution?: Evidence. We do not have enough evidence to prosecute the offender. For instance, in offences related to Computer Crime Act, the police failed to provide us enough evidence. So far, there is no case prosecuted under Computer Crime Act although there are police reports about the crime. This is due to the investigation that leads to ‘grey area’ where the evidence gathered is not adequate and the police failed to identify the offender and his location. The police also do not have enough experts in investigating computer crime cases. We are also facing problem because the cyberlaw is general and not specified, and the investigation officer always facing problem in interpreting the cyberlaw. If an offence is not ended with prosecution it means that the investigation process is not completed, the police cannot identify the offender.

Did you attend any seminar or course regarding this type of crime?: Yes, I attended many courses regarding this matter. Usually talks were given by public prosecutors, lawyers, judges, computer companies from the U.S., from the Bukit Aman police, and even from the hackers. They share their view and experience to us. First of all, we need to understand computer jargons and systems, how the offenders exploit the systems’ weaknesses and what type of activity is considered as an offense. We need ongoing courses and seminars to update ourselves. This type of crime is still new to us.

Is there any collaboration with foreign office?: So far no. The collaboration is at the police level only and does not involve our office.

What does the Attorney General say about the current situation? (few offenders are prosecuted even though many cases were reported): He is not satisfied with the situation.
TRANSCRIPT OF INTERVIEW WITH ASP VICTOR SANJOS, HEAD OF TECHNOLOGY CRIME INVESTIGATION UNIT ON 23 SEPTEMBER 2002.

What is the function of this unit?: Technology Crime Branch Unit (TCIU) carries out investigation to enforce Computer Crime Act and other acts. When there is intrusion and police report, we will open an investigation that is classified under Computer Crime Act (CCA).

Can you tell me about the structure of this unit?: TCIU is established in 1998 after the enforcement of CCA. Earlier, it has only two units, the investigation and forensic unit. The strength was only five people. Forensic unit then relocated to forensic lab. TCIU focuses only to investigation. It consists of four units – PC Investigation, Internet, R&D software, and interrogation. TCIU is under Department of Commercial Crime. The objectives of this unit are to enforce the CCA, conduct investigation, provides consultation service and expertise to the district and contingent investigation officers on how to obtain electronic evidence, provides assistance on investigation to other government agencies such as custom and foreign law enforcement agencies, and gives lectures about the enforcement of CCA to government agencies such as ILKAP and provides awareness program to the public.

What is the difference between investigation done by TCIU, NISER and MIMOS?: NISER does not have the authority to apprehend. They only carry out investigation to find out whether it is true or not the crime has been committed and then they will hand over the information to us for us to take further action in accordance to the existing law. We also hold discussion with them and ask their opinion when we are facing complex and intricate cases. But so far I found that local hackers' methods of attacks are still not so sophisticated. We act based on information. We conduct investigation when a police report is lodged. Then only we have the authority to investigate. That is the difference. We conduct investigation to detect, apprehend and prosecute them in court. We have cooperation with NISER. MIMOS is an ISP provider. When there is case a reported and it involves their service, we will contact them to seek for assistance in terms of information and etc, and we will give court order under section 5(1). This section provides us authority to obtain information.

What is the strength of this unit currently?: There are three officers (1 ASP and 2 Chief Inspectors), one detective corporal and two constables. However, we have 14 contingents, and from time to time we will train them. If there is a case reported in Sabah, for example, the Sabah state police contingent will open and conduct the investigation. If the case is complex, we will assist them and take over the case. We used to apprehend hacker red handed in year 2000. For now, there is no hardcore case, but there are many cases that involve defacement of reputation. Most cases are not reported because they consider the damage is not significant.
What is the success rate of solving the case?: There are many definitions of solving the case. First, when the case is closed or there is no case. Second, when a case is open, we identify the suspect and arrest him. Third, when the suspect is arrested and we prosecute him in court.

Are there any war games or simulations conducted?: No. We do not need such simulation because we are investigating many cases now.

Any profiling techniques done during investigation?: Yes.

Does TCIU have cooperation with foreign law enforcement agencies?: Yes especially with countries that have law similar to computer crime act.

Do you face any hurdles while having cooperation with them?: Yes. Some countries have data protection act that requires court order to get the info. Some of the info is regarded as sensitive for them. We depend on their discretion to get the info.

Do you face any challenge?: We face many challenges. Technology changes so fast and we have to follow and update ourselves by doing research. That is why we have our own R&D unit. The second challenge is cost. To ask for extra budget to buy new hardware, software and attending courses require procedure that consuming time. Third, state contingent police do not fully master the investigation techniques and we have to guide them from time to time. Fourth, deputy public prosecutors and judges also need to understand the technical aspect of this type of crime. Fifth, the CCA has flaws. Sixth, problem related to jurisdiction where Malaysia does not have extradition treaty with some countries. We cannot do anything to the offenders that launch their attack from these countries. We are also facing manpower problem where they need to have willingness and interest to involve in this type of investigation.

What is the latest development of the parliamentary web defacement case?: The case is still under investigation. We have sent our request to the law enforcement agency of a country where the hacker came from but they still do not reply to us.
TRANSCRIPT OF INTERVIEW WITH DEPUTY SUPERINTENDENT ABDUL AZIZ, AN ANALYST FROM COMPUTER CRIME FORENSIC LAB, ROYAL MALAYSIAN POLICE ON 1 OCTOBER 2002

What is the function of this unit?: Our function is to do computer analysis, examine and to find out any information related to the crime committed that is expected to be stored in the hard disk. We also give advice to our investigation officer on what can be done, should be done, and should not be done. We also educate them from time to time about the evidence gathering techniques. Besides that, we do analysis on evidence materials. Our analysis is nearly the same that is done by NISER but we are doing analysis on cases that are reported to the police and involve crime or have the elements of crime. We investigate not only cases under Computer Crime Act but also any case where computer is used to commit crime or computer is used to store information about the crime. NISER investigates only on cases that related to cyber laws.

How does this unit overcome the sophistication of attack techniques?: From time to time we are updating ourselves with information about new types of attack.

Any cooperation with foreign law enforcement agencies?: We have Interpol liaison to seek assistance from other countries. We often receive visitors from foreign law enforcement agencies such as Hong Kong, Australia to share experience and information on cyber crime cases.

What is the strength of this unit?: Three officers (1 Superintendent, 1 Deputy Superintendent, 1 Chief Inspector). We have to cover all over Malaysia. But at the same time we are educating state police contingents.

What is the challenge?: Sophistication of attack techniques requires us to study more to solve the case and it consumes time. From one course that I attended disclosed that there are more than 700 web sites that hosted free attack tools to be downloaded by anybody.

Is there any coordinated attack happened in Malaysia?: So far no.

Are there any war games or simulations conducted?: So far no.

How many cases have been brought to the attention of DPP? (Deputy Public Prosecutor): There are many cases that have been brought to the attention of DPP but we are a bit lucky because the moment we want to prosecute them, they pleaded guilty except one case where it is now under court proceeding. All of those cases are domestic originated attack.

What is the success rate of solving the case?: We have our own definition that we follow the Interpol standard. For us the moment we identified the suspect, we consider the case as solved.
Does your unit monitor the Internet? : We don’t monitor the Internet, on our level as CID. But the time will come where we have to do that. Now we are more reactive than proactive. We can only act when there is a police report. The report gives us authority to conduct investigation. One day we have to monitor the Internet and develop the capability but I don’t think we have enough manpower to conduct such operation. Nowadays most of the commercial crime committed using computer. We are upgrading the computer forensic capability especially to have more skillful and knowledgeable manpower. Computer crime is still new to us. We have only on case in court to test our expertise and capability to face defense council’s argument. We think we are doing the correct job by following international guideline but in court it will be different when lawyers ask technical questions.
NISER works in the context of advisory capacity, and it means we give professional advice from strategic, tactical and technical view, on to solve problem, on how to settle and handle them, how to cope with attacks if happens. We are like the early warning.

What type of warning: Any events that we think would give severe impact and people in Malaysia, for example last year the outbreak of Nimda and code red so we alerted public and various agencies in a serious and collaborative manner. We alerted them on the severity of attack and the need to react fast.

Besides that type of warning: We also study the national and international activities on anything to do with cyber security issues or information security issues, and we analyze what are the impacts on our nation, advice on implication of specific policies by international community and how to overcome it or what kind of initiative we should have in this country in order to protect this country from being labeled as incompetent not being able to manage information infrastructure and assets.

True, many of the information is open and accessible (open source), we browse through the internet and got lot of documents and issues articulated. I think is how well you analyze those information and how well you translate those information in a meaningful content, meaningful purpose.

Niser browse through the internet?: That is part of our job, we call it research, analyze it and give proposal to the government on what to do. As part of that we are also collaborating with other CERT around the world, we have connection with US cert, Australian cert, New Zealand CERT, Japan CERT, Singapore CERT and many other. We update each other on threats, new attacks that coming in and things in that nature.

We are focusing on technology assessment, meaning that what is the implication of specific technology and how does it impact us and do we analyze it in the security point of view.

How does NISER react with coordinated and widespread attack?: as usual, we will operate in a advisory capacity, we will inform various agencies that required to be informed and advise them what to do, and if needed, help them on doing it. NISER core business/core competent is on technology. We are able and competent in handling technology issues and able and competent to translate those technology requirement into strategic need and strategic value. We do not play the role of enforcement agency.

Neutral and impartial in our advice means that we give advice based on fact, numerical analysis, scientific findings, we don't advice on political and social ground.
If any attack comes to our country, we have the right to be concerned. The responsibility on protecting the information does not rely on us only, it falls on the owner. The owner must protect themselves first, before others can help. NISER will tell them that the problem is coming, if they don't know how to do and what to do, we can help on how to do and what to do. But in the end of the day, the owner of the information has to react upon those problems. So the responsibility in defending the nation from the cyber attack is not on us alone, its on everyone. We are not the first layer of defense. The first layer is the owner of the system itself, we can be called as experts views and reference centre. if we feel we need to alert, we will alert them but sometime we do not alert everybody on everything, there are things that we feel that "this is not serious". So we leave to respective agencies to handle it.

*How does NISER cooperate with law enforcement agencies?*: we help when there is a requirement. The principle here is we help not only to law enforcement agencies but also the government, community, home user, as many agencies and as many people as possible.

*How essential foreign collaboration to your work?*: it is very important, because in protecting our country, ourselves from cyberterrorism, collaborative model is the best model. Because at the end of the day it is about knowledge and competencies. These will be the front thing or the weapon. Knowledge and competency is in the mind of people, so how you leverage on these knowledge and competencies, other than cooperation and collaboration, i don't see any other means.

*What obstacle do you face?*: so far we do not face any obstacle yet, the only thing we may face is that the interpretation, different culture has different interpretation on some issues, but that does not mean that we can't cooperate, what we need to do is to understand their culture and what are important to them, and we sensitive about their culture and their need their priority and vice versa.

*NISER as firefighting?*: as I told you that it is not entirely in that way, firefighting is not our responsibility as well, it is the responsibility of the owner, if their information system is burning, then they have to do the firefighting, but we are handy to help, assist them in doing the firefighting effectively.

*Does NISER have a rapid reaction force?*: We don't call it rapid reaction force, we call it CERT. we have our computer emergency response team. If we need to dispatch our team on the ground, we will do that if necessary.

NISER shows a defensive posture, not offensive. Basically we have to follow our national philosophy, Malaysia as a whole adopt the policy of peaceful and believe on negotiation on table in a peaceful manner. I don't see any instances that Malaysia has been hostile or taking an offensive stance.
NISER is not entrusted as like the ministry of defense, we are only acting on advisory capacity for now. I don't know the government's moves in the coming years, as for now our position is acting on the advisory capacity. So meaning that, if someone need to be offensive, then it is not us, it is that agency who need to be offensive, we only provide them with expert advise and technical know how, until they are able to do it themselves. in summary, we advise them on how to make themselves capable, we believe in education and learning process, we don't believe in spoon feeding. The ultimate aim is to create self reliance at the end of the day. We are more favorable into the approach of upbringing.

CERT has 24-7 service, we have the mechanism to trigger us, and there are a lot of automated mechanisms. Most of the time its not out system who is being intruded, it is other people's system. They have to report to us through pager, email.

We have detection mechanism to alert us when there is a coordinated and widespread attack to this country.

NISER has limited firepower because it is always relative to evaluate.

NISER does not monitor the traffic because we don't have the power to do so. It is under other government agencies.

Has NISER encountered any coordinated attacks so far? : So far we do not have any record of that.

Can NISER withholds such attack? : I am very positive if various agencies collaborate, we can sustain the attack.

Any contingency plan if the attack breached certain level of security perimeter: as for now the contingency plan is left to the particular agencies to handle. Sure there is a contingency plan (within the context of national info structure)

Which agency will be the command and control center? : We have not designated any specific agency. I think there is no agency to do that for this moment. I think all the agencies can work together or can work within their own capacity (decentralized) to sustain the attack and we exchange information. When the crisis comes of course there will be somebody who will be given the task. In the even of attacks there will be an agency to be nominated to take in charge. The mechanism is there.

Does NISER conduct any war games? Not yet. It might be conducted in the future. NISER does not conduct any operation similar to Eligible Receiver.

How does NISER sniffing potential attack? : By assessing the network (pick up peculiarity), collaborating with other agencies in the country and overseas, exchanging information.
NSD (National Security Division) role is about policy matters. Information security is under MAMPU, NISER. But last year the government has decided to put it under National Information Security Committee (NISC), the newly established committee. This means that the low intensity threats have become middle level threat.

*NISC gives direction, control or coordinate*: We have not decided yet. For the time being, Infosec is still under MAMPU and NISER. We just set up our committee. But of course when it comes to NSD, it will become policy and we will monitor the agencies’ conformity to the policy. When we talk about NSD, it is all about policy. The way we make policy is we will gather all the threats that we are facing, then we will look into the strengths and weaknesses that we have. It will be the new guidance. From there we will make the policy. If the preceding policy that we handled to the agencies is sturdy, we won’t revamp but if there is a tendency of lower level threats becoming middle level, and middle level becoming high level threats, we will form new policies. Then it will be handled to the enforcement agencies for them to carry out. If within the agencies there are weaknesses about human resources, technologies, funding etc they will come back to us. NSD is not about operational, it is all policy matters.

*Does NSD gather all agencies to coordinate the defensive strategy?*: MAMPU will call them. But now (NISC) is established, NISC will call them to look into issues that arise to see whether our policy is adequate or do we need new policy.

*How would the country correspond to coordinated attack*: MAMPU and NISER will interdict the attack and they will inform the NISC about the situation. As long as the agencies able to handle the situation, they will take over the situation. If those agencies fail to interdict the attack, they will refer back to NISC. NISC will evaluate the input and devise strategies to interdict the attack. If they think the attack involves national security and needs direction, they will bring the situation to National Disaster and Relief Committee (NDRC). NDRC will mobilize all the available resources to interdict the attack.

However for now, NISC structure is still blur and we are still evaluating the situation. Strategic Committee will determine information warfare threats and the structure of NISC. We hope within next month we could come out with the threats list.

*What makes an activity or situation regarded as threat to national security*: First, it involves sovereignty. Second it injures public safety. Third, it agitates the law. Fourth it causes turmoil to the economy.

*What about joint defense operation between civilian agencies and military*: We have committees that comprised of military, police and civilian. Even within NSD we have military and police personnel.

137
A Glossary of ICT Terms

A
Algorithm
The term algorithm (pronounced AL-go-rith-um) is a procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. Al-Khwarizmi's work is the likely source for the word algebra as well. A computer program can be viewed as an elaborate algorithm. In mathematics and computer science, an algorithm usually means a small procedure that solves a recurrent problem.

Analog
In telecommunications, an analog signal is one in which a base carrier's alternating current frequency is modified in some way, such as by amplifying the strength of the signal or varying the frequency, in order to add information to the signal. Broadcast and telephone transmission have conventionally used analog technology. An analog signal can be represented as a series of sine waves. The term originated because the modulation of the carrier wave is analogous to the fluctuations of the human voice or other sound that is being transmitted.

Application
1) In information technology, an application is the use of a technology, system, or product.

2) The term application is a shorter form of application program. An application program is a program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of applications include word processors, database programs, Web browsers, development tools, drawing, paint, image editing programs, and communication programs. Applications use the services of the computer's operating system and other supporting applications.

Application Program Interface (API)
An application program interface (API - and sometimes spelled application programming interface) is the specific method prescribed by a computer operating system or by an application program by which a programmer writing an application program can make requests of the operating system or another application. An API can be contrasted with a graphical user interface or a command interface (both of which are direct user interfaces) as interfaces to an operating system or a program.

ASCII
ASCII (American Standard Code for Information Interchange) is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number (a string of seven 0s or 1s). 128 possible characters are defined.
ATM (asynchronous transfer mode)
ATM (asynchronous transfer mode) is a dedicated-connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path. Because ATM is designed to be easily implemented by hardware (rather than software), faster processing and switch speeds are possible. The prespecified bit rates are either 155.520 Mbps or 622.080 Mbps. Speeds on ATM networks can reach 10 Gbps.

B
Bandwidth
Bandwidth has a general meaning of how much information can be carried in a given time period (usually a second) over a wired or wireless communications link. For example, a link with a broad bandwidth - that is, a broadband link - is one that may be able to carry enough information to sustain the succession of images in a video presentation.

Band
In telecommunication, a band - sometimes called a frequency band - is a specific range of frequencies in the radio frequency (RF) spectrum, which is divided among ranges from very low frequencies (vlf) to extremely high frequencies (ehf). Each band has a defined upper and lower frequency limit. Because two radio transmitters sharing the same frequency band cause mutual interference, band usage is regulated. International use of the radio spectrum is regulated by the International Telecommunication Union (ITU). Domestic use of the radio spectrum is regulated by national agencies such as the Federal Communications Commission (Fcc) in the U.S. Regulatory organizations assign each transmission source a band of operation, a transmitter radiation pattern, and a maximum transmitter power.

Binary
Binary describes a numbering scheme in which there are only two possible values for each digit: 0 and 1. The term also refers to any digital encoding/decoding system in which there are exactly two possible states. In digital data memory, storage, processing, and communications, the 0 and 1 values are sometimes called "low" and "high," respectively.

Bit
A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1. Although computers usually provide instructions that can test and manipulate bits, they generally are designed to store data and execute instructions in bit multiples called bytes. In most computer systems, there are eight bits in a byte. The value of a bit is usually stored as either above or below a designated level of electrical charge in a single capacitor within a memory device.
In most computer systems, a byte is a unit of data that is eight binary digits long. A byte is the unit most computers use to represent a character such as a letter, number, or typographic symbol (for example, "g", "5", or "?"). A byte can also hold a string of bits that need to be used in some larger unit for application purposes (for example, the stream of bits that constitute a visual image for a program that displays images or the string of bits that constitutes the machine code of a computer program).

Boot
To boot (as a verb; also "to boot up") a computer is to load an operating system into the computer's main memory or random access memory (RAM). Once the operating system is loaded (and, for example, on a PC, you see the initial Windows or Mac desktop screen), it's ready for users to run applications. Sometimes you'll see an instruction to "reboot" the operating system. This simply means to reload the operating system (the most familiar way to do this on PCs is pressing the Ctrl, Alt, and Delete keys at the same time).

Broadband
In general, broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

Browser
A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse (navigate through and read) text files online.

Byte
In some computer systems, four bytes constitute a word, a unit that a computer processor can be designed to handle efficiently as it reads and processes each instruction. Some computer processors can handle two-byte or single-byte instructions. A byte is abbreviated with a "B". (A bit is abbreviated with a small "b".) Computer storage is usually measured in byte multiples. For example, an 820 MB hard drive holds a nominal 820 million bytes - or megabytes - of data. Byte multiples are based on powers of 2 and commonly expressed as a "rounded off" decimal number. For example, one megabyte ("one million bytes") is actually 1,048,576 (decimal) bytes. (Confusingly, however, some hard disk manufacturers and dictionary sources state that bytes for computer storage should be calculated as powers of 10 so that a megabyte really would be one million decimal bytes.)

BIOS
BIOS (basic input/output system) is the program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow
between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

C

Carrier
In information technology, a carrier (or carrier signal) is a transmitted electromagnetic pulse or wave at a steady base frequency of alternation on which information can be imposed by increasing signal strength, varying the base frequency, varying the wave phase, or other means.

Central Processing Unit (CPU)
CPU (central processing unit) is an older term for processor and microprocessor, the central unit in a computer containing the logic circuitry that performs the instructions of a computer's programs.

Cell
In wireless telephony, a cell is the geographical area covered by a cellular telephone transmitter. The transmitter facility itself is called the cell site. The cell provided by a cell site can be from one mile to twenty miles in diameter, depending on terrain and transmission power. Several coordinated cell sites are called a cell system. When you sign up with a cellular telephone service provider, you generally are given access to their cell system, which is essentially local. When travelling out of the range of this cell system, the cell system can enable you to be transferred to a neighboring company's cell system without your being aware of it.

Character
In information technology, a character is a printable symbol having phonetic or pictographic meaning and usually forming part of a word of text, depicting a numeral, or expressing grammatical punctuation. In information technology today, a character is generally one of a limited number of symbols, including the letters of a particular language's alphabet, the numerals in the decimal number system, and certain special symbols such as the ampersand (&) and "atsign" (@).

Ciphertext
Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result. A cipher (pronounced SAI-fuhr) is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself although here the term ciphertext is preferred. Its origin is the Arabic sifr, meaning empty or zero.

Computer
A computer is a device that accepts information (in the form of digital data) and manipulates it for some result based on a program or sequence of instructions on how data is to be processed. Complex computers also include the means for storing data
(including the program, which is also a form of data) for some necessary duration. A program may be invariable and built into the computer (and called logic circuitry as it is on microprocessors) or different programs may be provided to the computer (loaded into its storage and then started by an administrator or user). Today's computers have both kinds of programming.

**Common Gateway Interface (CGI)**
The common gateway interface (CGI) is a standard way for a Web server to pass a Web user's request to an application program and to receive data back to forward to the user. When the user requests a Web page (for example, by clicking on a highlighted word or entering a Web site address), the server sends back the requested page. However, when a user fills out a form on a Web page and sends it in, it usually needs to be processed by an application program. The Web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the Web's Hypertext Transfer Protocol (HTTP).

**Cryptology**
Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis. Since the cryptanalysis concepts are highly specialized and complex, we concentrate here only on some of the key mathematical concepts behind cryptography. In order for data to be secured for storage or transmission, it must be transformed in such a manner that it would be difficult for an unauthorized individual to be able to discover its true meaning. To do this, certain mathematical equations are used, which are very difficult to solve unless certain strict criteria are met. The level of difficulty of solving a given equation is known as its intractability. These types of equations form the basis of cryptography.

**Cryptography**
Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:
1) **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)
2) **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3) **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4) **Authentication** (the sender and receiver can confirm each others identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

**Cryptanalysis**

Cryptanalysis refers to the study of ciphers, ciphertext, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm. This is known as **breaking** the cipher, ciphertext, or cryptosystem. Breaking is sometimes used interchangeably with **weakening**. This refers to finding a property (fault) in the design or implementation of the cipher that reduces the number of keys required in a brute force attack (that is, simply trying every possible key until the correct one is found).

For example, assume that a symmetric cipher implementation uses a key length of $2^{128}$ bits (2 to the power of 128): this means that a brute force attack would need to try up to all $2^{128}$ possible combinations (rounds) to be certain of finding the correct key (or, on average, $2^{127}$ possible combinations) to convert the ciphertext into plaintext, which is not possible given present and near future computing abilities. However, a cryptanalysis of the cipher reveals a technique that would allow the plaintext to be found in $2^{40}$ rounds. While not completely broken, the cipher is now much weaker and the plaintext can be found with moderate computing resources.

**D**

**Data**

1) In computing, data is information that has been translated into a form that is more convenient to move or process. Relative to today’s computers and transmission media, data is information converted into binary digital form.

2) In computer component interconnection and network communication, data is often distinguished from "control information," "control bits," and similar terms to identify the main content of a transmission unit.

3) In telecommunications, data sometimes means digital-encoded information to distinguish it from analog-encoded information such as conventional telephone voice calls. In general, "analog" or voice transmission requires a dedicated continual connection for the duration of a related series of transmissions. Data transmission can often be sent with intermittent connections in packets that arrive in piecemeal fashion.

**Digital**

Digital describes electronic technology that generates, stores, and processes data in terms of two states: positive and non-positive. Positive is expressed or represented by the number 1 and non-positive by the number 0. Thus, data transmitted or stored with digital
technology is expressed as a string of 0's and 1's. Each of these state digits is referred to as a bit (and a string of bits that a computer can address individually as a group is a byte).

Prior to digital technology, electronic transmission was limited to analog technology, which conveys data as electronic signals of varying frequency or amplitude that are added to carrier waves of a given frequency. Broadcast and phone transmission has conventionally used analog technology. Digital technology is primarily used with new physical communications media, such as satellite and fiber optic transmission. A modem is used to convert the digital information in your computer to analog signals for your phone line and to convert analog phone signals to digital information for your computer.

Domain

1) In computing and telecommunication in general, a domain is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses.

2) On the Internet, a domain consists of a set of network addresses. This domain is organized in levels. The top level identifies geographic or purpose commonality (for example, the nation that the domain covers or a category such as "commercial"). The second level identifies a unique place within the top level domain and is, in fact, equivalent to a unique address on the Internet (an IP address). Lower levels of domain may also be used.

Domain Name

A domain name locates an organization or other entity on the Internet. For example, the domain name www.totalbaseball.com locates an Internet address for "totalbaseball.com" at Internet point 199.0.0.2 and a particular host server named "www". The "com" part of the domain name reflects the purpose of the organization or entity (in this example, "commercial") and is called the top-level domain name. The "totalbaseball" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name. The second-level domain name maps to and can be thought of as the "readable" version of the Internet address.

DOS

DOS (Disk Operating System) was the first widely-installed operating system for personal computers. (Earlier, the same name had been used for an IBM operating system for a line of business computers). The first personal computer version of DOS, called PC-DOS, was developed for IBM by Bill Gates and his new Microsoft Corporation. He retained the rights to market a Microsoft version, called MS-DOS. PC-DOS and MS-DOS are almost identical and most users have referred to either of them as just "DOS." DOS was (and still is) a non-graphical line-oriented command- or menu-driven operating system, with a relatively simple interface but not overly "friendly" user interface. Its prompt to enter a command looks like this:

C:>
The first Microsoft Windows operating system was really an application that ran on top of the MS-DOS operating system. Today, Windows operating systems continue to support DOS (or a DOS-like user interface) for special purposes by emulating the operating system. In the 1970s before the personal computer was invented, IBM had a different and unrelated DOS (Disk Operating System) that ran on smaller business computers. It was replaced by IBM's VSE operating system.

DMZ

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN "police action" in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed. Cisco, the leading maker of routers, is one company that sells products designed for setting up a DMZ.

E

Enterprise

In the computer industry, an enterprise is an organization that uses computers. A word was needed that would encompass corporations, small businesses, non-profit institutions, government bodies, and possibly other kinds of organizations. The term enterprise seemed to do the job. In practice, the term is applied much more often to larger organizations than smaller ones.

Encryption

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often
incorrectly called a "code," can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key. Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

F

File
In any computer system but especially in personal computers, a file is an entity of data available to system users (including the system itself and its application programs) that is capable of being manipulated as an entity (for example, moved from one file directory to another). The file must have a unique name within its own directory. Some operating systems and applications describe files with given formats by giving them a particular file name suffix. (The file name suffix is also known as a file name extension.) For example, a program or executable file is sometimes given or required to have an ".exe" suffix. In general, the suffixes tend to be as descriptive of the formats as they can within the limits of the number of characters allowed for suffixes by the operating system.

Firewall
Firewall is a system that is set up to control traffic flow between two networks. A firewall protects a computer network from unauthorized access. Firewalls may be hardware devices, software programs, or a combination of the two. A firewall typically guards an internal network against malicious access from the outside; however, firewalls may also be configured to limit access to the outside from internal users. A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.
Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources. Perhaps the most familiar form of Internet firewall is a proxy server. Proxy servers act as an intermediary between internal and external computers by receiving and selectively blocking data packets at the network boundary. These firewalls also provide an extra measure of safety by hiding internal LAN addresses from the outside. In a proxy server firewall environment, network requests from multiple clients appear to the outsider as all coming from the same proxy server address.

Frame
In telecommunications, a frame is data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data).

Frame Relay Network
Frame relay is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the end-points, which speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line, while the service provider figures out the route each frame travels to its destination and can charge based on usage. An enterprise can select a level of service quality - prioritizing some frames and making others less important.

Frequency
For an oscillating or varying current, frequency is the number of complete cycles per second in alternating current direction. The standard unit of frequency is the hertz, abbreviated Hz. If a current completes one cycle per second, then the frequency is 1 Hz; 60 cycles per second equals 60 Hz (the standard alternating-current utility frequency in some countries).

Gateway
A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.
Gbps
Gbps stands for billions of bits per second and is a measure of bandwidth on a digital data transmission medium such as optical fiber. With slower media and protocols, bandwidth may be in the Mbps (millions of bits or megabits per second) or the Kbps (thousands of bits or kilobits per second) range.

GUI (Graphical User Interface)
A GUI (usually pronounced GOO-ee) is a graphical (rather than purely textual) user interface to a computer. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text-and-keyboard oriented and usually consisted of commands you had to remember and computer responses that were infamously brief. The command interface of the DOS operating system (which you can still get to from your Windows operating system) is an example of the typical user-computer interface before GUIs arrived. An intermediate step in user interfaces between the command line interface and the GUI was the non-graphical menu-based interface, which let you interact by using a mouse rather than by having to type in keyboard commands.

H
Home page
For a Web user, the home page is the first Web page that is displayed after starting a Web browser like Netscape's Navigator or Microsoft's Internet Explorer. The browser is usually preset so that the home page is the first page of the browser manufacturer. However, you can set it to open to any Web site. For example, you can specify that "http://www.yahoo.com" or "http://whatis.com" be your home page. You can also specify that there be no home page (a blank space will be displayed) in which case you choose the first page from your bookmark list or enter a Web address.

Host
The term "host" is used in several contexts, in each of which it has a slightly different meaning:
1) In Internet protocol specifications, the term "host" means any computer that has full two-way access to other computers on the Internet. A host has a specific "local or host number" that, together with the network number, forms its unique IP address. If you use Point-to-Point Protocol to get access to your access provider, you have a unique IP address for the duration of any connection you make to the Internet and your computer is a host for that period. In this context, a "host" is a node in a network.

2) For companies or individuals with a Web site, a host is a computer with a Web server that serves the pages for one or more Web sites. A host can also be the company that provides that service, which is known as hosting.

3) In IBM and perhaps other mainframe computer environments, a host is a mainframe computer (which is now usually referred to as a "large server"). In this context, the
mainframe has intelligent or "dumb" workstations attached to it that use it as a host provider of services. (This does not mean that the host only has "servers" and the workstations only have "clients." The server/client relationship is a programming model independent of this contextual usage of "host.")

4) In other contexts, the term generally means a device or program that provides services to some smaller or less capable device or program.

Hosting
Hosting (also known as Web site hosting, Web hosting, and Webhosting) is the business of housing, serving, and maintaining files for one or more Web sites. More important than the computer space that is provided for Web site files is the fast connection to the Internet.

HTML (Hypertext Markup Language)
HTML (Hypertext Markup Language) is the set of codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. Each individual markup code is referred to as an element (but many people also refer to it as a tag). Some elements come in pairs that indicate when some display effect is to begin and when it is to end.

HTTP (Hypertext Transfer Protocol)
The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

Information
Information is stimuli that has meaning in some context for its receiver. When information is entered into and stored in a computer, it is generally referred to as data. After processing (such as formatting and printing), output data can again be perceived as information. When information is packaged or used for understanding or doing something, it is known as knowledge.

Intranet
An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the Wide Area Network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.
IP (Internet Protocol)
The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

An IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. On the Internet itself - that is, between the router that move packets from one point to another along the route - only the network part of the address is looked at.

The Internet is really the interconnection of many individual networks (it's sometimes referred to as an internetwork). So the Internet Protocol (IP) is basically the set of rules for one network communicating with any other (or occasionally, for broadcast messages, all other networks). Each network must know its own address on the Internet and that of any other networks with which it communicates. To be part of the Internet, an organization needs an Internet network number, which it can request from the Network Information Center (NIC). This unique network number is included in any packet sent out of the network onto the Internet.

In addition to the network address or number, information is needed about which specific machine or host in a network is sending or receiving a message. So the IP address needs both the unique network number and a host number (which is unique within the network). (The host number is sometimes called a local or machine address). An instruction is an order given to a computer processor by a computer program. At the lowest level, each instruction is a sequence of 0s and 1s that describes a physical operation the computer is to perform (such as "Add") and, depending on the particular instruction type, the
specification of special storage areas called registers that may contain data to be used in carrying out the instruction, or the location in computer memory of data.

ISP (Internet Service Provider)
An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building. Among the Malaysia ISPs are Tmnet, Jaring, Maxis.

K
Kilobyte
As a measure of computer memory or storage, a kilobyte (KB or Kbyte*) is approximately a thousand bytes (actually, 2 to the 10th power, or decimal 1,024 bytes).

L
LAN (Local Area Network)
A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

M
Mbps
Mbps stands for millions of bits per second or megabits per second and is a measure of bandwidth (the total information flow over a given time) on a telecommunications medium. Depending on the medium and the transmission method, bandwidth is also sometimes measured in the Kbps (thousands of bits or kilobits per second) range or the Gbps (billions of bits or gigabits per second) range. A megabit is a million binary pulses, or 1,000,000 (that is, 10^6) pulses (or "bits"). Some sources define a megabit to mean 1,048,576 (that is, 2^20) bits. Although the bit is a unit of the binary number system, bits in data communications are discrete signal pulses and have historically been counted using the decimal number system. For example, 28.8 kilobits per second (Kbps) is 28,800 bits per second. Because of computer architecture and memory address boundaries, bytes are always some multiple or exponent of two.

Memory
Memory is the electronic holding place for instructions and data that your computer's microprocessor can reach quickly. When your computer is in normal operation, its memory usually contains the main parts of the operating system and some or all of the
application programs and related data that are being used. Memory is often used as a shorter synonym for random access memory (RAM). This kind of memory is located on one or more microchips that are physically close to the microprocessor in your computer. Most desktop and notebook computers sold today include at least 16 megabytes of RAM, and are upgradeable to include more. The more RAM you have, the less frequently the computer has to access instructions and data from the more slowly accessed hard disk form of storage. Memory is sometimes distinguished from storage, or the physical medium that holds the much larger amounts of data that won’t fit into RAM and may not be immediately needed there. Storage devices include hard disks, floppy disks, CD-ROM, and tape backup systems. The terms auxiliary storage, auxiliary memory, and secondary memory have also been used for this kind of data repository.

Microprocessor
A microprocessor is a computer processor on a microchip. It's sometimes called a logic chip. It is the "engine" that goes into motion when you turn your computer on. A microprocessor is designed to perform arithmetic and logic operations that make use of small number-holding areas called registers. Typical microprocessor operations include adding, subtracting, comparing two numbers, and fetching numbers from one area to another. These operations are the result of a set of instructions that are part of the microprocessor design. When the computer is turned on, the microprocessor is designed to get the first instruction from the basic input/output system (BIOS) that comes with the computer as part of its memory. After that, either the BIOS, or the operating system that BIOS loads into computer memory, or an application program is "driving" the microprocessor, giving it instructions to perform.

Modem
A modem modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device.

N
Network
In information technology, a network is a series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.

Node
In a network, a node is a connection point, either a redistribution point or an end point for data transmissions. In general, a node has programmed or engineered capability to recognize and process or forward transmissions to other nodes.
Optical Fiber
Optical fiber (or "fiber optic") refers to the medium and the technology associated with the transmission of information as light pulses along a glass or plastic wire or fiber. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. Most telephone company long-distance lines are now of optical fiber.

Operating System
An operating system (sometimes abbreviated as "OS") is the program that, after being initially loaded into the computer by a boot program, manages all the other programs in a computer. The other programs are called applications or application programs. The application programs make use of the operating system by making requests for services through a defined application program interface (API). In addition, users can interact directly with the operating system through a user interface such as a command language or a graphical user interface (GUI).

An operating system performs these services for applications:
- In a multitasking operating system where multiple programs can be running at the same time, the operating system determines which applications should run in what order and how much time should be allowed for each application before giving another application a turn.
- It manages the sharing of internal memory among multiple applications.
- It handles input and output to and from attached hardware devices, such as hard disks, printers, and dial-up ports.
- It sends messages to each application or interactive user (or to a system operator) about the status of operation and any errors that may have occurred.
- It can offload the management of what are called batch jobs (for example, printing) so that the initiating application is freed from this work.
- On computers that can provide parallel processing, an operating system can manage how to divide the program so that it runs on more than one processor at a time.

All major computer platforms (hardware and software) require and sometimes include an operating system. Linux, Windows 2000, VMS, OS/400, AIX, and z/OS are all examples of operating systems.

Packet
A packet is the unit of data that is routed between an origin and a destination on the Internet.

Plaintext
In cryptography, plaintext is ordinary readable text before being encrypted into ciphertext or after being decrypted.
**Point-to-Point Protocol (PPP)**
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet service provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others).

**Protocol**
In information technology, a protocol (pronounced PROH-tuh-cahl, from the Greek *protocollon*, which was a leaf of paper glued to a manuscript volume, describing its contents) is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and each corresponding layer at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard. On the Internet, there are the TCP/IP protocols, consisting of:

- Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level
- Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level

**Program**
In computing, a program is a specific set of ordered operations for a computer to perform. In the modern computer that John von Neumann outlined in 1945, the program contains a one-at-a-time sequence of instructions that the computer follows. Typically, the program is put into a storage area accessible to the computer. The computer gets one instruction and performs it and then gets the next instruction. The storage area or memory can also contain the data that the instruction operates on. (Note that a program is also a special kind of "data" that tells how to operate on "application or user data").

Programs can be characterized as interactive or batch in terms of what drives them and how continuously they run. An interactive program receives data from an interactive user (or possibly from another program that simulates an interactive user). A batch program runs and does its work, and then stops. Batch programs can be started by interactive users who request their interactive program to run the batch program. A command interpreter or a Web browser is an example of an interactive program. A program that computes and prints out a company payroll is an example of a batch program. Print jobs are also batch programs.

**Processor**
A processor is the logic circuitry that responds to and processes the basic instructions that drive a computer. The term processor has generally replaced the term central processing
unit (CPU). The processor in a personal computer or embedded in small devices is often called a microprocessor.

Proxy Server
In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

PVC (Permanent Virtual Circuit)
A permanent virtual circuit (PVC) is a software-defined logical connection in a network such as a frame relay network. A feature of frame relay that makes it a highly flexible network technology is that users (companies or clients of network providers) can define logical connections and required bandwidth between end points and let the frame relay network technology worry about how the physical network is used to achieve the defined connections and manage the traffic.

R
RAM
RAM (random access memory) is the place in a computer where the operating system, application programs, and data in current use are kept so that they can be quickly reached by the computer's processor. RAM is much faster to read from and write to than the other kinds of storage in a computer, the hard disk, floppy disk, and CD-ROM. However, the data in RAM stays there only as long as your computer is running. When you turn the computer off, RAM loses its data. When you turn your computer on again, your operating system and other files are once again loaded into RAM, usually from your hard disk. RAM can be compared to a person's short-term memory and the hard disk to the long-term memory. The short-term memory focuses on work at hand, but can only keep so many facts in view at one time. If short-term memory fills up, your brain sometimes is able to refresh it from facts stored in long-term memory. A computer also works this way. If RAM fills up, the processor needs to continually go to the hard disk to overlay old data in RAM with new, slowing down the computer's operation. Unlike the hard disk which can become completely full of data so that it won't accept any more, RAM never runs out of memory. It keeps operating, but much more slowly than you may want it to.

Register
In a computer, a register is one of a small set of data holding places that are part of a computer microprocessor and that provide a place for passing data from one instruction to the next sequential instruction or to another program that the operating system has just given control to. A register must be large enough to hold an instruction - for example, in a 32-bit instruction computer, a register must be 32 bits in length. In some computer designs, there are smaller registers - for example, half-registers - for shorter instructions. Depending on the processor design and language rules, registers may be numbered or have arbitrary names.
Router
On the Internet, a router is a device or, in some cases, software in a computer, that
determines the next network point to which a packet should be forwarded toward its
destination. The router is connected to at least two networks and decides which way to
send each information packet based on its current understanding of the state of the
networks it is connected to. A router is located at any gateway (where one network meets
another).

S
Second-level Domain
A second-level domain (SLD) is the portion of a Uniform Resource Locator (URL) that
identifies the specific and unique administrative owner associated with an Internet
Protocol address (IP address). The second-level domain name includes the top-level
domain (top-level domain) name. For example, in:
whatis.com

"whatis" is a second-level domain. "whatis.com" is a second-level domain name (and
includes the top-level domain name of "com"). Second-level domains can be divided into
further domain levels. These subdomains sometimes represent different computer servers
within different departments. More than one second-level domain name can be used for
the same IP address.

Serial
Serial means one event at a time. It is usually contrasted with parallel, meaning more
than one event happening at a time. In data transmission, the techniques of time division
and space division are used, where time separates the transmission of individual bits of
information sent serially and space (on multiple lines or paths) can be used to have
multiple bits sent in parallel. In the context of computer hardware and data transmission:
serial connection, operation, and media usually indicate a simpler, slower operation and
parallel indicates a faster operation. This indication doesn't always hold since a serial
medium (for example, fiber optic cable) can be much faster than a slower medium that
carries multiple signals in parallel.

Server
In general, a server is a computer program that provides services to other computer
programs in the same or other computers.

Sine wave
A sine wave is a waveform is a representation of how alternating current (AC) varies
with time. The most familiar AC waveform is the sine wave, which derives its name from
the fact that the current or voltage varies with the sine of the elapsed time. Other common
AC waveforms are the square wave, the ramp, the sawtooth wave, and the triangular
wave.
Switch
In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.

TCP/IP
TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP. TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

Text
In information technology, text is a human-readable sequence of characters and the words they form that can be encoded into computer-readable formats. Text is usually distinguished from non-character encoded data, such as graphic images.

TLD (top-level domain)
On the Internet, a top-level domain (TLD) identifies the most general part of the domain name in an Internet address. A TLD is either a generic top-level domain (gTLD), such as "com" for "commercial," "edu" for "educational," and so forth, or a country code top-level domain (ccTLD), such as "fr" for France or "is" for Iceland or "my" for Malaysia.

Twisted pair
Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each connection on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable.
A URL (Uniform Resource Locator, previously Universal Resource Locator) - pronounced YU-AHR-EHL or, in some quarters, UHRL - is the address of a file (resource) accessible on the Internet. The type of file or resource depends on the Internet application protocol. Using the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP), the resource can be an HTML page (like the one you're reading), an image file, a program such as a common gateway interface application or Java applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and a pathname (hierarchical description of a file location) on the computer.

**URL** is a form of address that specifies the location of an object, usually a webpage or a website on the Internet. Here are some examples of URLs:

- http://abc.com.my
- mailto:someone@abc.com.my

A URL contains three parts, i.e.

- protocol (e.g. http, ftp, news, mailto)
- domain name of any Internet host (e.g. www.abc.com.my, abc.com, abc.com.my)
- path or file name (e.g. welcome.html, welcome/index.html, something.gz)

Therefore, a **domain name** is used in a URL. When you use the web or send an e-mail message, a domain name is used. For example,

- the URL http://www.abc.com.my contains the domain name abc.com.my
- the e-mail address somebody@abc.com.my contains the domain name abc.com.my

**source:** www.mynic.net

**VPN (Virtual Private Network)**

The more common method used today is with a Virtual Private Network between company sites. A VPN creates a secure path of communication over an insecure connection. It could also be considered a mechanism to connect hosts or networks such that they can communicate in a secure fashion, as though they were behind the same
firewall, while actually communicating over a public medium. A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

W

WAN (Wide Area Network)
A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.

Web server
A Web server is a program that serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a Web server program.

Wireless
Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

World Wide Web
A technical definition of the World Wide Web is: all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). "The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge." A Web site is a related collection of World Wide Web (WWW) files that includes a beginning file called a home page. A company or an individual tells you how to get to their Web site by giving you the address of their home page. From the home page, you can get to all the other pages on their site. For example, the Web site for IBM has the home page address of http://www.ibm.com.

Source:
searchnetworking.com
whatis.com
[accessed on 15 April 2003]