1

Introduction to Computer Architecture and Security

A Computer is composed of a number of different components:

Hardware: Computer hardware processes information by executing instructions, storing data, moving data among input and output devices, and transmitting and receiving information to and from remote network locations.

Software: Software consists of system software and application software or programs. Operating Systems such as Windows, UNIX/Linux and Snow Leopard are system software. Word, Firefox browser and iTunes are examples of application software.

Network: The network communication component is responsible for sending and receiving information and data through local area network or wireless connections.

Data is the fundamental representation of information and facts but usually formatted in a special way. All software is divided into two categories: data and programs. Programs are a collection of instructions for manipulating data.

Figure 1.1 shows a view of a computer system from a user perspective. Here a computer system no longer looks like an onion as traditional textbooks used to represent. Instead, a network component (including hardware and software) is added as a highway for data flowing in and out of the computer system.

Computer architecture is to study how to design computer systems. It includes all components: the central processing unit (CPU), computer memory and storage, input and output devices (I/O), and network components.

Since the invention of the Internet, computer systems are no longer standalone machines. The traditional "computing" concept of the single machine model is

Computer Architecture and Security: Fundamentals of Designing Secure Computer Systems, First Edition.
Shuangbao (Paul) Wang and Robert S. Ledley.

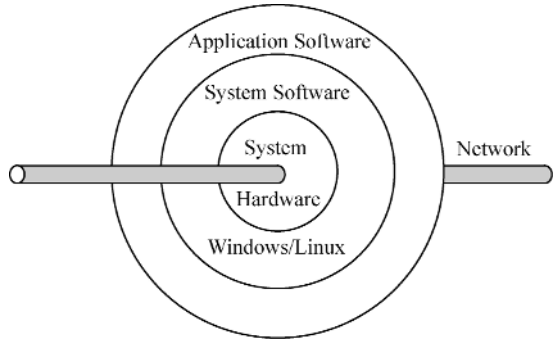

Figure 1.1 A conceptual diagram of a common computer system

fading away. For most users, information exchange has taken an important role in everyday computer uses.

As computer systems expose themselves over the Internet, the threat to computer systems has grown greater and greater. To protect a computer system (hardware, software, network, and data) from attacks, people have developed many counter-attack techniques such as firewalls, intrusion detection systems, user authentications, data encryptions and so on.

Despite the numerous efforts to prevent attacks, the threat to computer systems is far from over. Computer compromises and data bleach are still very common. If you look back to those counter-attack techniques, most of the detection systems are based on passive techniques. They only work after attacks have taken place.

A firewall by its name is a wall to prevent fire from spreading. On the other hand, it also likes a dam or levee to prevent flood. People can build a dam or levee high enough to protect against flood. However nobody can predict how high the water level will be. The 2005 New Orleans levee leak caused by Katrina is an example of this.

In medicine, people spent billions of dollars to develop new drugs to cure illness. However ancient Chinese people study how to eat well and exercise well to prevent illness. This is the same as now the so-called prevention medicine. If we apply the same mechanism to computer systems, we draw the conclusion that we not only need to build firewalls, more importantly we need to develop computer systems that are immune from attacks.

In early 2005, a US patent was filed to propose new technology that can prevent hackers from getting information stored in computer systems. The technology has drawn the attention of industry, academia, as well as government.

Figure 1.2 shows a conceptual diagram of the proposed secured computer system. Note that in addition to the traditional hardware and software, the system added an additional layer. It is like a sandbox that "separates" the computer system from the outside world. In this book, we call it a virtual semi-conductor or semi "network

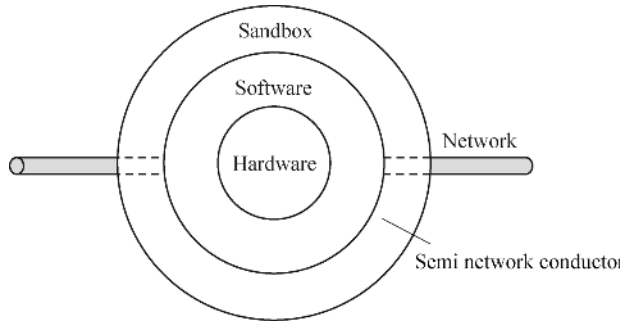

Figure 1.2 A conceptual diagram of a secured computer system

conductor." It allows the computer operator to control information and data access so that hackers are no longer able to steal data from the computer system. We will discuss this in more detail in the following chapters.

Computer Architecture and Security will teach you how to design secured computer systems. It includes information on how to secure central processing unit (CPU) memory, buses, input/output interfaces. Moreover, the book explains how to secure computer architecture as a whole so that modern computers can be built on the new architecture free of data breaches.

1.1 History of Computer Systems

Computers originally mean to compute or to calculate. The earliest computing devices date back more than two thousand years. The abacus (second century BC) which was introduced in China is one of them.

Blaise Pascal, a renowned French scientist and philosopher, invented a mechanical adding machine in 1645. Gottfried Leibniz invented the first calculator in 1694. The multiplication could be performed by repeated turns of a handle, and by shifting the position of the carriage relative to the accumulator. In December 26, 1837, Charles Babbage proposed a calculating engine that is capable of solving mathematical problems including addition, subtraction, multiplication, division, and finding the square root.

Herman Hollerith, a German-American statistician and the founder of the company that became IBM, developed a punched-card electric tabulating machine in 1889. The first program-controlled computing machine is the German machine Z3 which was developed in 1941. Mark-I, also known as IBM automatic sequence-controlled calculator, was developed by Howard Aiken at Harvard University in 1944. The Electronic Numerical Integrator and Calculator (ENIAC) was developed in May 1943. The machine was used to calculate bomb trajectories and to develop hydrogen bombs. It was not a stored-program machine, a key way to distinguish between earlier computing devices and modern computers.

The final step toward developing a modern computer was characterized as follows:

- General-purpose. The computer can be used by anybody in any domain.
- Electronic. The computer is controlled by electronic signals instead of mechanical devices.
- Stored-program. Programs are stored in its internal memory so they can run automatically without much human interaction.
- Computation. The computer can take numerical quantities to compute.

There are other features such as it has the ability for a program to read and modify itself during the course of a computation, using registers to store temporary data, indirect addressing and so on.

Professor John von Neumann, of the Institute for Advanced Study at Princeton University, one of the leading mathematicians of his time, developed a stored-program electronic computer in 1945. It is generally accepted that the first documented discussion of the advantages of using just one large internal memory, in which instructions as well as data could be held, was the draft report on EDVAC written by Neumann, dated June 30, 1945. (The full report is available on www.wiley.com/go/wang/comp_arch)

Since 1945, the Neumann computer architecture has been the foundation of modern computers, a CPU, memory and storage, input/output devices, a bus with address, data and control signals that connects the components.

Early computers were made of vacuum tubes. They are large and consume a great deal of energy. During the mid 1950s to early 1960s, solid-state transistors were used and in the mid 1960s to early 1970s, integrated circuits (IC) were used in computers. Minicomputer PDP-11 in 1970, supercomputer CDC (Cray) and mainframe IBM 360 are some examples of computers during that time. Intel 8080 and Zilog Z80 are 8-bit processors made of large-scale IC. Later, Intel's 8086 (16-bit), 80286 (16-bit) and Motorola's 68000 (16/32-bit) made of very large-scale IC (VLSI) opened the era of so-called microcomputers.

The uses of microcomputers were greatly increased by the software development. UNIX and MS-DOS later became Windows are still being used as operating systems (system software) today. Word processing, spreadsheets and databases, and many other application programs help people to carry out office works. Fortran, C, Java and many other computer languages assist software developers to program new software applications.

Now computers have grown from single-chip processors to multiple processors (cores) such as dual-cores, quad-cores and eight-cores in the near future. On the other hand, smaller devices or handheld devices such as pads and smart cell phones have the ability to handle information and data needs for many people.

With virtualization technology, a "guest" or virtual operating system may run as a process on a "host" or physical computer system. It is often considered as "computers on a computer."

Now, network connections have become an essential part of a computer system. People have developed many ways to enhance the security of computer architecture from protecting CPU and memory to building "firewalls" to detect intrusions. The study of computer architecture with security as a whole was not started until recently. This book aims to provide readers with the latest developments in designing modern computer systems that are immune from attacks.

1.1.1 Timeline of Computer History

The timeline of computer history (Computer History, 2012) covers the most important advancements in computer research and development during 1939 to 1988.

1939: Hewlett-Packard is founded. David Packard and Bill Hewlett founded Hewlett-Packard in a Palo Alto, California garage. Their first product was the HP 200A Audio Oscillator, which rapidly became a popular piece of test equipment for engineers. Walt Disney Pictures ordered eight of the 200B models to use as sound effects generators for the 1940 movie "Fantasia."

1940: The Complex Number Calculator (CNC) is completed. In 1939, Bell Telephone Laboratories completed this calculator, designed by researcher George Stibitz. In 1940, Stibitz demonstrated the CNC at an American Mathematical Society conference held at Dartmouth College. Stibitz stunned the group by performing calculations remotely on the CNC (located in New York City) using a Teletype connected via special telephone lines. This is considered to be the first demonstration of remote access computing.

1941: Konrad Zuse finishes the Z3 computer. The Z3 was an early computer built by German engineer Konrad Zuse working in complete isolation from developments elsewhere. Using 2,300 relays, the Z3 used floating point binary arithmetic and had a 22-bit word length. The original Z3 was destroyed in a bombing raid of Berlin in late 1943. However, Zuse later supervised a reconstruction of the Z3 in the 1960s which is currently on display at the Deutsches Museum in Munich.

1942: The Atanasoff-Berry Computer (ABC) is completed. After successfully demonstrating a proof-of-concept prototype in 1939, Atanasoff received funds to build the full-scale machine. Built at Iowa State College (now University), the ABC was designed and built by Professor John Vincent Atanasoff and graduate student Cliff Berry between 1939 and 1942. The ABC was at the center of a patent dispute relating to the invention of the computer, which was resolved in 1973 when it was shown that ENIAC co-designer John Mauchly had come to examine the ABC shortly after it became functional.

The legal result was a landmark: Atanasoff was declared the originator of several basic computer ideas, but the computer as a concept was declared

un-patentable and thus was freely open to all. This result has been referred to as the "dis-invention of the computer." A full-scale reconstruction of the ABC was completed in 1997 and proved that the ABC machine functioned as Atanasoff had claimed.

1943: Project Whirlwind begins. During World War II, the US Navy approached the Massachusetts Institute of Technology (MIT) about building a flight simulator to train bomber crews. The team first built a large analog computer, but found it inaccurate and inflexible. After designers saw a demonstration of the ENIAC computer, they decided on building a digital computer. By the time the Whirlwind was completed in 1951, the Navy had lost interest in the project, though the US Air Force would eventually support the project which would influence the design of the SAGE program.

The Relay Interpolator is completed. The US Army asked Bell Labs to design a machine to assist in testing its M-9 Gun Director. Bell Labs mathematician George Stibitz recommended using a relay-based calculator for the project. The result was the Relay Interpolator, later called the Bell Labs Model II. The Relay Interpolator used 440 relays and since it was programmable by paper tape, it was used for other applications following the war.

1944: Harvard Mark-1 is completed. Conceived by Harvard professor Howard Aiken, and designed and built by IBM, the Harvard Mark-1 was a room-sized, relay-based calculator. The machine had a 50 ft long camshaft that synchronized the machine's thousands of component parts. The Mark-1 was used to produce mathematical tables but was soon superseded by stored program computers.

The first Colossus is operational at Bletchley Park. Designed by British engineer Tommy Flowers, the Colossus was designed to break the complex Lorenz ciphers used by the Nazis during WWII. A total of ten Colossi were delivered to Bletchley, each using 1,500 vacuum tubes and a series of pulleys transported continuous rolls of punched paper tape containing possible solutions to a particular code. Colossus reduced the time to break Lorenz messages from weeks to hours. The machine's existence was not made public until the 1970s.

1945: **John von Neumann** wrote "First Draft of a Report on the EDVAC" in which he outlined the architecture of a stored-program computer. Electronic storage of programming information and data eliminated the need for the more clumsy methods of programming, such as punched paper tape – a concept that has characterized mainstream computer development since 1945. Hungarian-born von Neumann demonstrated prodigious expertise in hydrodynamics, ballistics, meteorology, game theory, statistics, and the use of mechanical devices for computation. After the war, he concentrated on the development of Princeton's Institute for Advanced Studies computer and its copies around the world.

1946: In February, the public got its first glimpse of the ENIAC, a machine built by John Mauchly and J. Presper Eckert that improved by 1,000 times on the speed of its contemporaries.

- *Start of project*: 1943
- *Completed*: 1946
- *Programmed*: plug board and switches
- *Speed*: 5,000 operations per second
- *Input/output*: cards, lights, switches, plugs
- *Floor space*: 1,000 square feet
- *Project leaders*: John Mauchly and J. Presper Eckert.

An inspiring summer school on computing at the University of Pennsylvania's Moore School of Electrical Engineering stimulated construction of stored-program computers at universities and research institutions. This free, public set of lectures inspired the EDSAC, BINAC, and, later, IAS machine clones like the AVIDAC. Here, Warren Kelleher completes the wiring of the arithmetic unit components of the AVIDAC at Argonne National Laboratory. Robert Dennis installs the inter-unit wiring as James Woody Jr. adjusts the deflection control circuits of the memory unit.

1948: IBM's Selective Sequence Electronic Calculator computed scientific data in public display near the company's Manhattan headquarters. Before its decommissioning in 1952, the SSEC produced the moon-position tables used for plotting the course of the 1969 Apollo flight to the moon.

- *Speed:* 50 multiplications per second
- *Input/output:* cards, punched tape
- *Memory type:* punched tape, vacuum tubes, relays
- *Technology:* 20,000 relays, 12,500 vacuum tubes
- *Floor space:* 25 feet by 40 feet
- *Project leader:* Wallace Eckert.

1949: Maurice Wilkes assembled the EDSAC, the first practical stored-program computer, at Cambridge University. His ideas grew out of the Moore School lectures he had attended three years earlier.

For programming the EDSAC, Wilkes established a library of short programs called subroutines stored on punched paper tapes.

- *Technology:* vacuum tubes
- *Memory:* 1 K words, 17 bits, mercury delay line
- *Speed:* 714 operations per second.

The Manchester Mark I computer functioned as a complete system using the Williams tube for memory. This university machine became the prototype for Ferranti Corp.'s first computer.

- *Start of project:* 1947
- *Completed:* 1949
- *Add time:* 1.8 microseconds
- *Input/output:* paper tape, teleprinter, switches
- *Memory size:* 128 + 1024 40-digit words
- *Memory type:* cathode ray tube, magnetic drum
- *Technology:* 1,300 vacuum tubes
- *Floor space:* medium room
- *Project leaders:* Frederick Williams and Tom Kilburn.

1950: Engineering Research Associates of Minneapolis built the ERA 1101, the first commercially produced computer; the company's first customer was the US Navy. It held 1 million bits on its magnetic drum, the earliest magnetic storage devices. Drums registered information as magnetic pulses in tracks around a metal cylinder. Read/write heads both recorded and recovered the data. Drums eventually stored as many as 4,000 words and retrieved any one of them in as little as five-thousandths of a second.

The National Bureau of Standards constructed the Standards Eastern Automatic Computer (SEAC) in Washington as a laboratory for testing components and systems for setting computer standards. The SEAC was the first computer to use all-diode logic, a technology more reliable than vacuum tubes, and the first stored-program computer completed in the United States. Magnetic tape in the external storage units (shown on the right of this photo) stored programming information, coded subroutines, numerical data, and output.

The National Bureau of Standards completed its SWAC (Standards Western Automatic Computer) at the Institute for Numerical Analysis in Los Angeles. Rather than testing components like its companion, the SEAC, the SWAC had an objective of computing using already-developed technology.

1951: MIT's Whirlwind debuted on Edward R. Murrow's "See It Now" television series. Project director Jay Forrester described the computer as a "reliable operating system," running 35 hours a week at 90% utility using an electrostatic tube memory.

- *Start of project:* 1945
- *Completed:* 1951
- *Add time:* 0.05 microseconds
- *Input/output:* cathode ray tube, paper tape, magnetic tape
- *Memory size:* 2048 16-digit words
- *Memory type:* cathode ray tube, magnetic drum, tape (1953 – core memory)
- *Technology:* 4,500 vacuum tubes, 14,800 diodes
- *Floor space:* 3,100 square feet
- *Project leaders:* Jay Forrester and Robert Everett.

1952: John von Neumann's IAS computer became operational at the Institute for Advanced Studies in Princeton, N.J. Contract obliged the builders to share their designs with other research institutes. This resulted in a number of clones: the MANIAC at Los Alamos Scientific Laboratory, the ILLIAC at the University of Illinois, the Johnniac at Rand Corp., the SILLIAC in Australia, and others.

1953: IBM shipped its first electronic computer, the 701. During three years of production, IBM sold 19 machines to research laboratories, aircraft companies, and the federal government.

1954: The IBM 650 magnetic drum calculator established itself as the first mass-produced computer, with the company selling 450 in one year. Spinning at 12,500 rpm, the 650s magnetic data-storage drum allowed much faster access to stored material than drum memory machines.

1956: MIT researchers built the TX-0, the first general-purpose, programmable computer built with transistors. For easy replacement, designers placed each transistor circuit inside a "bottle," similar to a vacuum tube. Constructed at MIT's Lincoln Laboratory, the TX-0 moved to the MIT Research Laboratory of Electronics, where it hosted some early imaginative tests of programming, including a Western movie shown on TV, 3-D tic-tac-toe, and a maze in which mice found martinis and became increasingly inebriated.

1958: SAGE – Semi-Automatic Ground Environment – linked hundreds of radar stations in the United States and Canada in the first large-scale computer communications network. An operator directed actions by touching a light gun to the screen.

The air defense system operated on the AN/FSQ-7 computer (known as Whirlwind II during its development at MIT) as its central computer. Each computer used a full megawatt of power to drive its 55,000 vacuum tubes, 175,000 diodes and 13,000 transistors.

1959: IBM's 7000 series mainframes were the company's first transistorized computers. At the top of the line of computers – all of which emerged significantly faster and more dependable than vacuum tube machines – sat the 7030, also known as the "Stretch." Nine of the computers, which featured a 64-bit word and other innovations, were sold to national laboratories and other scientific users. L. R. Johnson first used the term "architecture" in describing the Stretch.

1960: The precursor to the minicomputer, DEC's PDP-1 sold for $120,000. One of 50 built, the average PDP-1 included with a cathode ray tube graphic display, needed no air conditioning and required only one operator. It's large scope intrigued early hackers at MIT, who wrote the first computerized video game, SpaceWar!, for it. The SpaceWar! creators then used the game as a standard demonstration on all 50 computers.

1961: According to Datamation magazine, IBM had an 81.2% share of the computer market in 1961, the year in which it introduced the 1400 Series. The 1401 mainframe, the first in the series, replaced the vacuum tube with smaller, more reliable transistors and used a magnetic core memory.

Demand called for more than 12,000 of the 1401 computers, and the machine's success made a strong case for using general-purpose computers rather than specialized systems.

1962: The LINC (Laboratory Instrumentation Computer) offered the first real time laboratory data processing. Designed by Wesley Clark at Lincoln Laboratories, Digital Equipment Corp. later commercialized it as the LINC-8.

Research faculty came to a workshop at MIT to build their own machines, most of which they used in biomedical studies. DEC supplied components.

1964: IBM announced the System/360, a family of six mutually compatible computers and 40 peripherals that could work together. The initial investment of $5 billion was quickly returned as orders for the system climbed to 1,000 per month within two years. At the time IBM released the System/360, the company was making a transition from discrete transistors to integrated circuits, and its major source of revenue moved from punched-card equipment to electronic computer systems.

CDC's 6600 supercomputer, designed by Seymour Cray, performed up to 3 million instructions per second – a processing speed three times faster than that of its closest competitor, the IBM Stretch. The 6600 retained the distinction of being the fastest computer in the world until surpassed by its successor, the CDC 7600, in 1968. Part of the speed came from the computer's design, which had 10 small computers, known as peripheral processors, funneling data to a large central processing unit.

1965: Digital Equipment Corp. introduced the PDP-8, the first commercially successful minicomputer. The PDP-8 sold for $18,000, one-fifth the price of a small IBM 360 mainframe. The speed, small size, and reasonable cost enabled the PDP-8 to go into thousands of manufacturing plants, small businesses, and scientific laboratories.

1966: The Department of Defense Advanced Research Projects Agency contracted with the University of Illinois to build a large parallel processing computer, the ILLIAC IV, which did not operate until 1972 at NASA's Ames Research Center. The first large-scale array computer, the ILLIAC IV achieved a computation speed of 200 million instructions per second, about 300 million operations per second, and 1 billion bits per second of I/O transfer via a unique combination of parallel architecture and the overlapping or "pipe-lining" structure of its 64 processing elements.

This photograph shows one of the ILLIAC's 13 Burroughs disks, the debugging computer, the central unit, and the processing unit cabinet with a processing element.

Hewlett-Packard entered the general purpose computer business with its HP-2115 for computation, offering a computational power formerly found only in much larger computers. It supported a wide variety of languages, among them Basic, ALGOL, and Fortran.

1968: Data General Corp., started by a group of engineers that had left Digital Equipment Corp., introduced the Nova, with 32 kilobytes of memory, for $8,000.

The simple architecture of the Nova instruction set inspired Steve Wozniak's Apple I board eight years later.

The Apollo Guidance Computer made its debut orbiting the Earth on Apollo 7. A year later, it steered Apollo 11 to the lunar surface. Astronauts communicated with the computer by punching two-digit codes and the appropriate syntactic category into the display and keyboard unit.

1971: The Kenbak-1, the first personal computer, advertised for $750 in *Scientific American*. Designed by John V. Blankenbaker using standard medium-scale and small-scale integrated circuits, the Kenbak-1 relied on switches for input and lights for output from its 256-byte memory. In 1973, after selling only 40 machines, Kenbak Corp. closed its doors.

1972: Hewlett-Packard announced the HP-35 as "a fast, extremely accurate electronic slide rule" with a solid-state memory similar to that of a computer. The HP-35 distinguished itself from its competitors by its ability to perform a broad variety of logarithmic and trigonometric functions, to store more intermediate solutions for later use, and to accept and display entries in a form similar to standard scientific notation.

1973: The TV Typewriter, designed by Don Lancaster, provided the first display of alphanumeric information on an ordinary television set. It used $120 worth of electronics components, as outlined in the September 1973 issue of *Radio Electronics*. The original design included two memory boards and could generate and store 512 characters as 16 lines of 32 characters. A 90-minute cassette tape provided supplementary storage for about 100 pages of text.

The Micral was the earliest commercial, non-kit personal computer based on a micro-processor, the Intel 8008. Thi Truong developed the computer and Philippe Kahn the software. Truong, founder and president of the French company R2E, created the Micral as a replacement for minicomputers in situations that didn't require high performance. Selling for $1,750, the Micral never penetrated the US market. In 1979, Truong sold Micral to Bull.

1974: Researchers at the Xerox Palo Alto Research Center designed the Alto – the first work station with a built-in mouse for input. The Alto stored several files simultaneously in windows, offered menus and icons, and could link to a local area network. Although Xerox never sold the Alto commercially, it gave a number of them to universities. Engineers later incorporated its features into work stations and personal computers.

1975: The January edition of *Popular Electronics* featured the Altair 8800 computer kit, based on Intel's 8080 microprocessor, on its cover. Within weeks of the computer's debut, customers inundated the manufacturing company, MITS, with orders. Bill Gates and Paul Allen licensed Basic as the software language for the Altair. Ed Roberts invented the 8800 – which sold for $297, or $395 with a case – and coined the term "personal computer." The machine came with 256 bytes of memory (expandable to 64 K) and an open 100-line bus structure that evolved into

the S-100 standard. In 1977, MITS sold out to Pertec, which continued producing Altairs through 1978.

1976: Steve Wozniak designed the Apple I, a single-board computer. With specifications in hand and an order for 100 machines at $500 each from the Byte Shop, he and Steve Jobs got their start in business. In this photograph of the Apple I board, the upper two rows are a video terminal and the lower two rows are the computer. The 6502 microprocessor in the white package sits on the lower right. About 200 of the machines sold before the company announced the Apple II as a complete computer.

The Cray I made its name as the first commercially successful vector processor. The fastest machine of its day, its speed came partly from its shape, a C, which reduced the length of wires and thus the time signals needed to travel across them.

- *Project started:* 1972
- *Project completed:* 1976
- *Speed:* 166 million floating-point operations per second
- *Size:* 58 cubic feet
- *Weight:* 5,300 lbs.
- *Technology:* Integrated circuit
- *Clock rate:* 83 million cycles per second
- *Word length:* 64-bit words
- *Instruction set:* 128 instructions.

1977: The Commodore Personal Electronic Transactor (PET) – the first of several personal computers released in 1977 – came fully assembled and was straightforward to operate, with either 4 or 8 kilobytes of memory, two built-in cassette drives, and a membrane "chiclet" keyboard.

The Apple II became an instant success when released in 1977 with its printed circuit motherboard, switching power supply, keyboard, case assembly, manual, game paddles, A/C powercord, and cassette tape with the computer game "Breakout." When hooked up to a color television set, the Apple II produced brilliant color graphics.

In the first month after its release, Tandy Radio Shack's first desktop computer – the TRS-80 – sold 10,000 units, well more than the company's projected sales of 3,000 units for one year. Priced at $599.95, the machine included a Z80 based microprocessor, a video display, 4 kilobytes of memory, Basic, cassette storage, and easy-to-understand manuals that assumed no prior knowledge on the part of the consumer.

1978: The VAX 11/780 from Digital Equipment Corp. featured the ability to address up to 4.3 gigabytes of virtual memory, providing hundreds of times the capacity of most minicomputers.

1979: Atari introduces the Model 400 and 800 Computer. Shortly after delivery of the Atari VCS game console, Atari designed two microcomputers with game capabilities: the Model 400 and Model 800. The two machines were built with the idea

that the 400 would serve primarily as a game console while the 800 would be more of a home computer. Both sold well, though they had technical and marketing problems, and faced strong competition from the Apple II, Commodore PET, and TRS-80 computers.

1981: IBM introduced its PC, igniting a fast growth of the personal computer market. The first PC ran on a 4.77 MHz Intel 8088 microprocessor and used Microsoft's MS-DOS operating system.

Adam Osborne completed the first portable computer, the Osborne I, which weighed 24 pounds and cost $1,795. The price made the machine especially attractive, as it included software worth about $1,500. The machine featured a 5-inch display, 64 kilobytes of memory, a modem, and two 5 1/4-inch floppy disk drives.

Apollo Computer unveiled the first work station, its DN100, offering more power than some minicomputers at a fraction of the price. Apollo Computer and Sun Microsystems, another early entrant in the work station market, optimized their machines to run the computer-intensive graphics programs common in engineering.

1982: The Cray XMP, first produced in this year, almost doubled the operating speed of competing machines with a parallel processing system that ran at 420 million floating-point operations per second, or megaflops. Arranging two Crays to work together on different parts of the same problem achieved the faster speed. Defense and scientific research institutes also heavily used Crays.

Commodore introduces the Commodore 64. The C64, as it was better known, sold for $595, came with 64KB of RAM and featured impressive graphics. Thousands of software titles were released over the lifespan of the C64. By the time the C64 was discontinued in 1993, it had sold more than 22 million units and is recognized by the 2006 Guinness Book of World Records as the greatest selling single computer model of all time.

1983: Apple introduced its Lisa. The first personal computer with a graphical user interface, its development was central in the move to such systems for personal computers. The Lisa's sloth and high price ($10,000) led to its ultimate failure.

The Lisa ran on a Motorola 68000 microprocessor and came equipped with 1 megabyte of RAM, a 12-inch black-and-white monitor, dual 5 1/4-inch floppy disk drives and a 5 megabyte Profile hard drive. The Xerox Star – which included a system called Smalltalk that involved a mouse, windows, and pop-up menus – inspired the Lisa's designers.

Compaq Computer Corp. introduced the first PC clone that used the same software as the IBM PC. With the success of the clone, Compaq recorded first-year sales of $111 million, the most ever by an American business in a single year.

With the introduction of its PC clone, Compaq launched a market for IBM-compatible computers that by 1996 had achieved an 83% share of the personal computer market. Designers reverse-engineered the Compaq clone, giving it nearly 100% compatibility with the IBM.

1984: Apple Computer launched the Macintosh, the first successful mouse-driven computer with a graphic user interface, with a single $1.5 million commercial during the 1984 Super Bowl. Based on the Motorola 68000 microprocessor, the Macintosh included many of the Lisa's features at a much more affordable price: $2,500.

Apple's commercial played on the theme of George Orwell's "1984" and featured the destruction of Big Brother with the power of personal computing found in a Macintosh. Applications that came as part of the package included MacPaint, which made use of the mouse, and MacWrite, which demonstrated WYSIWYG (What You See Is What You Get) word processing.

IBM released its PC Jr. and PC-AT. The PC Jr. failed, but the PC-AT, several times faster than original PC and based on the Intel 80286 chip, claimed success with its notable increases in performance and storage capacity, all for about $4,000. It also included more RAM and accommodated high-density 1.2-megabyte 5 1/4-inch floppy disks.

1985: The Amiga 1000 is released. Commodore's Amiga 1000 sold for $1,295 dollars (without monitor) and had audio and video capabilities beyond those found in most other personal computers. It developed a very loyal following and add-on components allowed it to be upgraded easily. The inside of the case is engraved with the signatures of the Amiga designers, including Jay Miner as well as the paw print of his dog Mitchy.

1986: Daniel Hillis of Thinking Machines Corp. moved artificial intelligence a step forward when he developed the controversial concept of massive parallelism in the Connection Machine. The machine used up to 65,536 processors and could complete several billion operations per second. Each processor had its own small memory linked with others through a flexible network that users could alter by reprogramming rather than rewiring.

The machine's system of connections and switches let processors broadcast information and requests for help to other processors in a simulation of brainlike associative recall. Using this system, the machine could work faster than any other at the time on a problem that could be parceled out among the many processors.

IBM and MIPS released the first RISC-based workstations, the PC/RT and R2000-based systems. Reduced instruction set computers grew out of the observation that the simplest 20% of a computer's instruction set does 80% of the work, including most base operations such as add, load from memory, and store in memory.

The IBM PC-RT had 1 megabyte of RAM, a 1.2-megabyte floppy disk drive, and a 40-megabyte hard drive. It performed 2 million instructions per second, but other RISC-based computers worked significantly faster.

1987: IBM introduced its PS/2 machines, which made the 3 1/2-inch floppy disk drive and video graphics array standard for IBM computers. The first IBMs to include Intel's 80386 chip, the company had shipped more than 1 million units by the end of the year. IBM released a new operating system, OS/2, at the same time, allowing the use of a mouse with IBMs for the first time.

1988: Apple cofounder Steve Jobs, who left Apple to form his own company, unveiled the NeXT. The computer he created failed but was recognized as an important innovation. At a base price of $6,500, the NeXT ran too slowly to be popular.

The significance of the NeXT rested in its place as the first personal computer to incorporate a drive for an optical storage disk, a built-in digital signal processor that allowed voice recognition, and object-oriented languages to simplify programming. The NeXT offered Motorola 68030 microprocessors, 8 megabytes of RAM, and a 256-megabyte read/write optical disk storage.

The milestones during this period are: the stored program computer architecture proposed by John von Neumann in 1945; the first transistorized computer IBM 7000 series in 1958; IBM 360 in 1964; the first vector processor Cray I in 1976; Apple II in 1977; IBM-PC in 1981; Apple Macintosh in 1984; the first RISC-based workstation IBM PC/RT in 1986.

Innovation and commercialization are the main characteristics during this 50 year period.

1.1.2 Timeline of Internet History

The timeline of Internet history covers most important advancements in Internet research and development from year 1962 to 1992.

1962: At MIT, a wide variety of computer experiments are going on. Ivan Sutherland uses the TX-2 to write Sketchpad, the origin of graphical programs for computer-aided design.

J.C.R. Licklider writes memos about his Intergalactic Network concept, where everyone on the globe is interconnected and can access programs and data at any site from anywhere. He is talking to his own "Intergalactic Network" of researchers across the country. In October, "Lick" becomes the first head of the computer research program at ARPA, which he calls the Information Processing Techniques Office (IPTO).

Leonard Kleinrock completes his doctoral dissertation at MIT on queuing theory in communication networks, and becomes an assistant professor at UCLA.

The SAGE (Semi Automatic Ground Environment), based on earlier work at MIT and IBM, is fully deployed as the North American early warning system. Operators of "weapons directing consoles" use a light gun to identify moving objects that show up on their radar screens. SAGE sites are used to direct air defense. This project provides experience in the development of the SABRE air travel reservation system and later air traffic control systems.

1963: Licklider starts to talk with Larry Roberts of Lincoln Labs, director of the TX-2 project, Ivan Sutherland, a computer graphics expert whom he has hired to work at ARPA and Bob Taylor, who joins ARPA in 1965. Lick contracts with MIT, UCLA, and BBN to start work on his vision.

Syncom, the first synchronous communication satellite, is launched. NASA's satellite is assembled in the Hughes Aircraft Company's facility in Culver City, California. Total payload is 55 pounds.

A joint industry-government committee develops American Standard Code for Information Interchange (ASCII), the first universal standard for computers. It permits machines from different manufacturers to exchange data. 128 unique 7-bit strings stand for either a letter of the English alphabet, one of the Arabic numerals, one of an assortment of punctuation marks and symbols, or a special function, such as the carriage return.

1964: Simultaneous work on secure packet switching networks is taking place at MIT, the RAND Corporation, and the National Physical Laboratory in Great Britain. Paul Baran, Donald Davies, Leonard Kleinrock, and others proceed in parallel research. Baran is one of the first to publish, *On Data Communications Networks.* Kleinrock's thesis is also published as a seminal text on queuing theory.

IBM's new System 360 computers come onto the market and set the de facto worldwide standard of the 8-bit byte, making the 12-bit and 36-bit word machines almost instantly obsolete. The $5 billion investment by IBM into this family of six mutually compatible computers pays off, and within two years orders for the System 360 reach 1,000 per month.

On-line transaction processing debuts with IBM's SABRE air travel reservation system for American Airlines. SABRE (Semi-Automatic Business Research Environment) links 2,000 terminals in sixty cities via telephone lines.

Licklider leaves ARPA to return to MIT, and Ivan Sutherland moves to IPTO. With IPTO funding, MIT's Project MAC acquires a GE-635 computer and begins the development of the Multics timesharing operating system.

1965: DEC unveils the PDP-8, the first commercially successful minicomputer. Small enough to sit on a desktop, it sells for $18,000 – one-fifth the cost of a low-end IBM/360 mainframe. The combination of speed, size, and cost enables the establishment of the minicomputer in thousands of manufacturing plants, offices, and scientific laboratories.

With ARPA funding, Larry Roberts and Thomas Marill create the first wide-area network connection. They connect the TX-2 at MIT to the Q-32 in Santa Monica via a dedicated telephone line with acoustic couplers. The system confirms the suspicions of the Intergalactic Network researchers that telephone lines work for data, but are inefficient, wasteful of bandwidth, and expensive. As Kleinrock predicts, packet switching offers the most promising model for communication between computers.

Late in the year, Ivan Sutherland hires Bob Taylor from NASA. Taylor pulls together the ideas about networking that are gaining momentum among IPTO's computer-scientist contractors.

The ARPA-funded JOSS (Johnniac Open Shop System) at the RAND Corporation goes on line. The JOSS system permits online computational problem solving at a number of remote electric typewriter consoles. The standard IBM Model 868

electric typewriters are modified with a small box with indicator lights and activating switches. The user input appears in green, and JOSS responds with the output in black.

1966: Taylor succeeds Sutherland to become the third director of IPTO. In his own office, he has three different terminals, which he can connect by telephone to three different computer systems research sites around the nation. Why can't they all talk together? His problem is a metaphor for that facing the ARPA computer research community.

Taylor meets with Charles Herzfeld, the head of ARPA, to outline his issues. Twenty minutes later he has a million dollars to spend on networking. The idea is to link all the IPTO contractors. After several months of discussion, Taylor persuades Larry Roberts to leave MIT to start the ARPA network program.

Simultaneously, the English inventor of packet switching, Donald Davies, is theorizing at the British National Physical Laboratory (NPL) about building a network of computers to test his packet switching concepts.

Honeywell introduces the DDP-516 minicomputer and demonstrates its ruggedness with a sledgehammer. This catches Roberts' eye.

1967: Larry Roberts convenes a conference in Ann Arbor, Michigan, to bring the ARPA researchers together. At the conclusion, Wesley Clark suggests that the network be managed by interconnected "Interface Message Processors" in front of the major computers. Called IMPs, they evolve into today's routers.

Roberts puts together his plan for the ARPANET. The separate strands of investigation begin to converge. Donald Davies, Paul Baran, and Larry Roberts become aware of each other's work at an ACM conference where they all meet. From Davies, the word "packet" is adopted and the proposed line speed in ARPANET is increased from 2.4 Kbps to 50 Kbps.

The acoustically coupled modem, invented in the early 1960s, is vastly improved by John van Geen of the Stanford Research Institute (SRI). He introduces a receiver that can reliably detect bits of data amid the hiss heard over long-distance telephone connections.

1968: Roberts and the ARPA team refine the overall structure and specifications for the ARPANET. They issue an RFQ for the development of the IMPs.

At Bolt, Beranek and Newman (BBN), Frank Heart leads a team to bid on the project. Bob Kahn plays a major role in shaping the overall BBN designs. BBN wins the project in December.

Roberts works with Howard Frank and his team at Network Analysis Corporation designing the network topology and economics. Kleinrock's team prepares the network measurement system at UCLA, which is to become the site of the first node.

The ILLIAC IV, the largest supercomputer of its time, is being built at Burroughs under a NASA contract. More than 1,000 transistors are squeezed onto its RAM chip, manufactured by the Fairchild Semiconductor Corporation, yielding 10 times the speed at one-hundredth the size of equivalent core memory.

ILLIAC-IV will be hooked to the ARPANET so that remote scientists can have access to its unique capabilities.

1969: Frank Heart puts a team together to write the software that will run the IMPs and to specify changes in the Honeywell DDP-516 they have chosen. The team includes Ben Barker, Bernie Cosell, Will Crowther, Bob Kahn, Severo Ornstein, and Dave Walden.

Four sites are selected. At each, a team gets to work on producing the software to enable its computers and the IMP to communicate. At UCLA, the first site, Vint Cerf, Steve Crocker, and Jon Postel work with Kleinrock to get ready. On April 7, Crocker sends around a memo entitled "Request for Comments." This is the first of thousands of RFCs that document the design of the ARPANET and the Internet.

The team calls itself the Network Working Group (RFC 10), and comes to see its job as the development of a "protocol," the collection of programs that comes to be known as NCP (Network Control Protocol).

The second site is the Stanford Research Institute (SRI), where Doug Engelbart saw the ARPA experiment as an opportunity to explore wide-area distributed collaboration, using his NLS system, a prototype "digital library." SRI supported the Network Information Center, led by Elizabeth (Jake) Feinler and Don Nielson.

At the University of California, Santa Barbara (UCSB) Glen Culler and Burton Fried investigate methods for display of mathematical functions using storage displays to deal with the problem of screen refresh over the net. Their investigation of computer graphics supplies essential capabilities for the representation of scientific information.

After installation in September, handwritten logs from UCLA show the first host-to-host connection, from UCLA to SRI, is made on October 29, 1969. The first "Log-In" crashes the SRI host, but the next attempt works!

1970: Nodes are added to the ARPANET at the rate of one per month.

Programmers Dennis Ritchie and Kenneth Thompson at Bell Labs complete the UNIX operating system on a spare DEC minicomputer. UNIX combines many of the time-sharing and file-management features offered by Multics and wins a wide following, particularly among scientists.

Bob Metcalfe builds a high-speed (100 Kbps) network interface between the MIT IMP and a PDP-6 to the ARPANET. It runs for 13 years without human intervention. Metcalfe goes on to build another ARPANET interface for Xerox PARC's PDP-10 clone (MAXC).

DEC announces the Unibus for its PDP-11 minicomputers to allow the addition and integration of myriad computer-cards for instrumentation and communications.

In December, the Network Working Group (NWG) led by Steve Crocker finishes the initial ARPANET Host-to-Host protocol, called the Network Control Protocol (NCP).

1971: The ARPANET begins the year with 14 nodes in operation. BBN modifies and streamlines the IMP design so it can be moved to a less cumbersome platform

than the DDP-516. BBN also develops a new platform, called a Terminal Interface Processor (TIP) which is capable of supporting input from multiple hosts or terminals.

The Network Working Group completes the Telnet protocol and makes progress on the file transfer protocol (FTP) standard. At the end of the year, the ARPANET contains 19 nodes as planned.

Intel's release of the 4004, the first "computer on a chip," ushers in the epoch of the microprocessor. The combination of memory and processor on a single chip reduces size and cost, and increases speed, continuing the evolution from vacuum tube to transistor to integrated circuit.

Many small projects are carried out across the new network, including the demonstration of an aircraft-carrier landing simulator. However, the overall traffic is far lighter than the network's capacity. Something needs to stimulate the kind of collaborative and interactive atmosphere consistent with the original vision. Larry Roberts and Bob Kahn decide that it is time for a public demonstration of the ARPANET. They choose to hold this demonstration at the International Conference on Computer Communication (ICCC) to be held in Washington, DC, in October 1972.

1972: The ARPANET grows by ten more nodes in the first 10 months of 1972. The year is spent finishing, testing, and releasing all the network protocols, and developing network demonstrations for the ICCC.

At BBN, Ray Tomlinson writes a program to enable electronic mail to be sent over the ARPANET. It is Tomlinson who develops the "user@host" convention, choosing the @ sign arbitrarily from the non-alphabetic symbols on the keyboard. Unbeknownst to him, @ is already in use as an escape character, prompt, or command indicator on many other systems. Other networks will choose other conventions, inaugurating a long period known as the e-mail "header wars." Not until the late 1980s will "@" finally become a worldwide standard.

Following the lead of Intel's 4004 chip, hand-held calculators ranging from the simple Texas Instruments four-function adding machines to the elaborate Hewlett-Packard scientific calculators immediately consign ordinary slide rules to oblivion.

Xerox PARC develops a program called Smalltalk, and Bell Labs develops a language called "C."

Steve Wozniak begins his career by building one of the best-known "blue boxes;" tone generators that enable long-distance dialing while bypassing the phone company's billing equipment.

The ICCC demonstrations are a tremendous success. One of the best known demos features a conversation between ELIZA, Joseph Weizenbaum's artificially-intelligent psychiatrist located at MIT, and PARRY, a paranoid computer developed by Kenneth Colby at Stanford. Other demos feature interactive chess games, geography quizzes, and an elaborate air traffic control simulation. An AT&T delegation visits ICCC but leaves in puzzlement.

1973: Thirty institutions are connected to the ARPANET. The network users range from industrial installations and consulting firms like BBN, Xerox PARC and the MITRE Corporation, to government sites like NASA's Ames Research Laboratories, the National Bureau of Standards, and Air Force research facilities.

The ICCC demonstrations prove packet-switching a viable technology, and ARPA (now DARPA, where the "D" stands for "Defense") looks for ways to extend its reach. Two new programs begin: Packet Radio sites are modeled on the ALOHA experiment at the University of Hawaii designed by Norm Abramson, connecting seven computers on four islands; and a satellite connection enables linking to two foreign sites in Norway and the UK.

Bob Kahn moves from BBN to DARPA to work for Larry Roberts, and his first self-assigned task is the interconnection of the ARPANET with other networks. He enlists Vint Cerf, who has been teaching at Stanford. The problem is that ARPANET, radio-based PRnet, and SATNET all have different interfaces, packet sizes, labeling, conventions and transmission rates. Linking them together is very difficult.

Kahn and Cerf set about designing a net-to-net connection protocol. Cerf leads the newly formed International Network Working Group. In September 1973, the two give their first paper on the new Transmission Control Protocol (TCP) at an INWG meeting at the University of Sussex in England.

Meanwhile, at Xerox PARC, Bob Metcalfe is working on a wire-based system modeled on ALOHA protocols for Local Area Networks (LANs). It will become Ethernet.

1974: Ethernet is demonstrated by networking Xerox PARC's new Alto computers.

BBN recruits Larry Roberts to direct a new venture, called Telenet, which is the first public packet-switched service. Roberts' departure creates a crisis in the DARPA IPTO office.

DARPA has fulfilled its initial mission. Discussions about divesting DARPA of operational responsibility for the network are held. Because it is DARPA-funded, BBN has no exclusive right to the source code for the IMPs. Telenet and other new networking enterprises want BBN to release the source code. BBN argues that it is always changing the code and that it has recently undergone a complete rewrite at the hands of John McQuillan. Their approach makes Roberts' task of finding a new director for IPTO difficult. J.C.R. Licklider agrees to return to IPTO from MIT on a temporary basis.

In addition to DARPA, The National Science Foundation (NSF) is actively supporting computing and networking at almost 120 universities. The largest NSF installation is at the National Center for Atmospheric Research (NCAR) in Boulder, Colorado. There, scientists use a home-built "remote job entry" system to connect to NCAR's CDC 7600 from major universities.

Bob Kahn and Vint Cerf publish "A Protocol for Packet Network Interconnection" in the May 1974 issue of IEEE Transactions on Communications Technology. Shortly thereafter, DARPA funds three contracts to develop and implement the Kahn-Cerf Transmission Control Protocol (TCP) protocol described in their paper, one at Stanford (Cerf and his students), one at BBN (Ray Tomlinson), and one at University College London (directed by Peter Kirstein and his students).

Daily traffic on the ARPANET exceeds 3 million packets.

1975: The ARPANET geographical map now shows 61 nodes. Licklider arranges its administration to be turned over to the Defense Communications Agency (DCA). BBN remains the contractor responsible for network operations. BBN agrees to release the source code for IMPs and TIPs.

The Network Working Group maintains its open system of discussion via RFCs and e-mail lists. Discomfort grows with the bureaucratic style of DCA.

The Department of Energy creates its own net to support its own research. This net operates over dedicated lines connecting each site to the computer centers at the National Laboratories.

NASA begins planning its own space physics network, SPAN. These networks have connections to the ARPANET so the newly developed TCP protocol begins to get a workout. Internally, however, the new networks use such a variety of protocols that true interoperability is still an issue.

1976: DARPA supports computer scientists at UC Berkeley who are revising a Unix system to incorporate TCP/IP protocols. Berkeley Unix also incorporates a second set of Bell Labs protocols, called UUCP, for systems to use dial-up connections.

Seymour Cray demonstrates the first vector-processor supercomputer, the CRAY-1. The first customers include Lawrence Livermore National Laboratory, Los Alamos National Laboratory, and NCAR. The CRAY-1 hardware is more compact and faster than previous supercomputers. No wire is more than 4 feet long, and the clock period is 12.5 nanoseconds (billionths of a second). The machine is cooled by freon circulated through stainless steel tubing bonded within vertical wedges of aluminum between the stacks of circuit boards (Cray patents the bonding process). The CRAY-1's speed and power attract researchers who want access to it over networks.

Vint Cerf moves from Stanford to DARPA to work with Bob Kahn on networking and the TCP/IP protocols.

1977: Steve Wozniak and Steve Jobs announce the Apple II computer. Also introduced are the Tandy TRS-80 and the Commodore Pet. These three off-the-shelf machines create the consumer and small business markets for computers.

Cerf and Kahn mount a major demonstration, "internetting" among the Packet Radio net, SATNET, and the ARPANET. Messages go from a van in the Bay Area across the US on ARPANET, then to University College London and back via satellite to Virginia, and back through the ARPANET to the University of Southern California's Information Sciences Institute. This shows its applicability to international deployment.

Larry Landweber of the University of Wisconsin creates THEORYNET providing e-mail between over 100 researchers and linking elements of the University of Wisconsin in different cities via a commercial packet service like Telenet.

1978: The appearance of the first very small computers and their potential for communication via modem to dial up services starts a boom in a new set of niche industries, like software and modems.

Vint Cerf at DARPA continues the vision of the Internet, forming an International Cooperation Board chaired by Peter Kirstein of University College London, and an Internet Configuration Control Board, chaired by Dave Clark of MIT.

The ARPANET experiment formally is complete. This leaves an array of boards and task forces over the next few years trying to sustain the vision of a free and open Internet that can keep up with the growth of computing.

1979: Larry Landweber at Wisconsin holds a meeting with six other universities to discuss the possibility of building a Computer Science Research Network to be called CSNET. Bob Kahn attends as an advisor from DARPA, and Kent Curtis attends from NSF's computer research programs. The idea evolves over the summer between Landweber, Peter Denning (Purdue), Dave Farber (Delaware), and Tony Hearn (Utah).

In November, the group submits a proposal to NSF to fund a consortium of eleven universities at an estimated cost of $3 million over five years. This is viewed as too costly by the NSF.

USENET starts a series of shell scripts written by Steve Bellovin at UNC to help communicate with Duke. Newsgroups start with a name that gives an idea of its content. USENET is an early example of a client server where users dial in to a server with requests to forward certain newsgroup postings. The server then "serves" the request.

1980: Landweber's proposal has many enthusiastic reviewers. At an NSF-sponsored workshop, the idea is revised in a way that both wins approval and opens up a new epoch for NSF itself. The revised proposal includes many more universities. It proposes a three-tiered structure involving ARPANET, a TELENET-based system, and an e-mail only service called PhoneNet. Gateways connect the tiers into a seamless whole. This brings the cost of a site within the reach of the smallest universities. Moreover, NSF agrees to manage CSNET for two years, after which it will turn it over to the University Corporation for Atmospheric Research (UCAR), which is made up of more than fifty academic institutions.

The National Science Board approves the new plan and funds it for five years at a cost of $5 million. Since the protocols for interconnecting the subnets of CSNET include TCP/IP, NSF becomes an early supporter of the Internet.

NASA has ARPANET nodes, as do many Department of Energy (DOE) sites. Now several Federal agencies support the Internet, and the number is growing.

Research by David Patterson at Berkeley and John Hennessy at Stanford promotes "reduced instruction set" computing. IBM selects the disk operating system DOS, developed by Microsoft, to operate its planned PC.

1981: By the beginning of the year, more than 200 computers in dozens of institutions have been connected in CSNET. BITNET, another startup network, is based on protocols that include file transfer via e-mail rather than by the FTP procedure of the ARPA protocols.

The Internet Working Group of DARPA publishes a plan for the transition of the entire network from the Network Control Protocol to the Transmission Control Protocol/ Internet Protocol (TCT/IP) protocols developed since 1974 and already in wide use (RFC 801).

At Berkeley, Bill Joy incorporates the new TCP/IP suite into the next release of the Unix operating system. The first "portable" computer is launched in the form of the Osborne, a 24-pound suitcase-sized device.

The IBM PC is launched in August 1981.

Meanwhile, Japan mounts a successful challenge to US chip makers by producing 64-kbit chips so inexpensively that US competitors charge the chips are being "dumped" on the US market.

1982: *Time Magazine* names "the computer" its "Man of the Year." Cray Research announces plans to market the Cray X-MP system in place of the Cray-1. At the other end of the scale, the IBM PC "clones" begin appearing.

An NSF panel chaired by the Courant Institute's Peter Lax reports that US scientists lack access to supercomputers. It contains the testimony of University of Illinois astrophysicist Larry Smarr that members of his discipline have been forced to travel to Germany to use American-made supercomputers.

The period during which *ad hoc* networking systems have flourished has left TCP/IP as only one contender for the title of "standard." Indeed, the International Organization for Standards (ISO) has written and is pushing ahead with a "reference" model of an interconnection standard called Open Systems Interconnection (OSI) – already adopted in preliminary form for interconnecting DEC equipment. But while OSI is a standard existing for the most part on paper, the combination of TCP/IP and the local area networks created with Ethernet technology are driving the expansion of the living Internet.

Drew Major and Kyle Powell write Snipes, an action game to be played on PCs over the network. They package the game as a "demo" for a PC software product from SuperSet Software, Inc. This is the beginning of Novell.

Digital Communications Associates introduces the first coaxial cable interface for micro-to-mainframe communications.

1983: In January, the ARPANET standardizes on the TCP/IP protocols adopted by the Department of Defense (DOD). The Defense Communications Agency decides to split the network into a public "ARPANET" and a classified "MILNET," with only 45 hosts remaining on the ARPANET. Jon Postel issues an RFC assigning numbers to the various interconnected nets. Barry Leiner takes Vint Cerf's place at DARPA, managing the Internet.

Numbering the Internet hosts and keeping tabs on the host names simply fails to scale with the growth of the Internet. In November, Jon Postel and Paul Mockapetris

of USC/ISI and Craig Partridge of BBN develop the Domain Name System (DNS) and recommend the use of the now familiar user@host.domain addressing system.

The number of computers connected via these hosts is much larger, and the growth is accelerating with the commercialization of Ethernet.

Having incorporated TCP/IP into Berkeley Unix, Bill Joy is key to the formation of Sun Microsystems. Sun develops workstations that ship with Berkeley Unix and feature built-in networking. At the same time, the Apollo workstations ship with a special version of a token ring network.

In July 1983, an NSF working group, chaired by Kent Curtis, issues a plan for "A National Computing Environment for Academic Research" to remedy the problems noted in the Lax report. Congressional hearings result in advice to NSF to undertake an even more ambitious plan to make supercomputers available to US scientists.

1984: In January, Apple announces the Macintosh. Its user-friendly interface swells the ranks of new computer users.

Novelist William Gibson coins the term cyberspace in *Neuromancer*, a book that adds a new genre to science fiction and fantasy.

The newly developed DNS is introduced across the Internet, with the now familiar domains of .gov, .mil, .edu, .org, .net, and .com. A domain called .int, for international entities, is not much used. Instead, hosts in other countries take a two-letter domain indicating the country. The British JANET explicitly announces its intention to serve the nation's higher education community, regardless of discipline.

Most important for the Internet, NSF issues a request for proposals to establish supercomputer centers that will provide access to the entire US research community, regardless of discipline and location. A new division of Advanced Scientific Computing is created with a budget of $200 million over five years.

Datapoint, the first company to offer networked computers, continues in the marketplace, but fails to achieve critical mass.

1985: NSF announces the award of five supercomputing center contracts:

- Cornell Theory Center (CTC), directed by Nobel laureate Ken Wilson.
- The John Von Neumann Center (JVNC) at Princeton, directed by computational fluid dynamicist Steven Orszag.
- The National Center for Supercomputing Applications (NCSA), directed at the University of Illinois by astrophysicist Larry Smarr.
- The Pittsburgh Supercomputing Center (PSC), sharing locations at Westinghouse, the University of Pittsburgh, and Carnegie Mellon University, directed by Michael Levine and Ralph Roskies.
- The San Diego Supercomputer Center (SDSC), on the campus of the University of California, San Diego, and administered by the General Atomics Company under the direction of nuclear engineer Sid Karin.

By the end of 1985, the number of hosts on the Internet (all TCP/IP interconnected networks) has reached 2,000.

MIT translates and publishes *Computers and Communication* by Dr. Koji Kobayashi, the Chairman of NEC. Dr. Kobayashi, who joined NEC in 1929, articulates his clear vision of "C & C," the integration of computing and communication.

1986: The 56 Kbps backbone between the NSF centers leads to the creation of a number of regional feeder networks – JVNCNET, NYSERNET, SURANET, SDSCNET and BARRNET – among others. With the backbone, these regionals start to build a hub and spoke infrastructure. This growth in the number of interconnected networks drives a major expansion in the community including the DOE, DOD and NASA.

Between the beginning of 1986 and the end of 1987 the number of networks grows from 2,000 to nearly 30,000.

TCP/IP is available on workstations and PCs such as the newly introduced Compaq portable computer. Ethernet is becoming accepted for wiring inside buildings and across campuses. Each of these developments drives the introduction of terms such as bridging and routing and the need for readily available information on TCP/IP in workshops and manuals. Companies such as Proteon, Synoptics, Banyan, Cabletron, Wellfleet, and Cisco emerge with products to feed this explosion.

At the same time, other parts of the US Government and many of the traditional computer vendors mount an attempt to validate their products being built to the OSI theoretical specifications, in the form of the Corporation for Open Systems.

USENET starts a major shakeup which becomes known as the "Great Renaming." A driving force is that, as many messages are traveling over ARPANET, desirable new news groups such as "alt.sex" and "alt.drugs" are not allowed.

1987: The NSF, realizing the rate and commercial significance of the growth of the Internet, signs a cooperative agreement with Merit Networks which is assisted by IBM and MCI. Rick Adams co-founds UUNET to provide commercial access to UUCP and the USENET newsgroups, which are now available for the PC. BITNET and CSNET also merge to form CREN.

The NSF starts to implement its T1 backbone between the supercomputing centers with 24 RT-PCs in parallel implemented by IBM as "parallel routers." The T1 idea is so successful that proposals for T3 speeds in the backbone begin.

In early 1987 the number of hosts passes 10,000 and by year-end there have been over 1,000 RFCs issued.

Network management starts to become a major issue and it becomes clear that a protocol is needed between routers to allow remote management. SNMP is chosen as a simple, quick, near term solution.

1988: The upgrade of the NSFNET backbone to T1 completes and the Internet starts to become more international with the connection of Canada, Denmark, Finland, France, Iceland, Norway and Sweden.

In the US more regionals spring up – Los Nettos and CERFnet both in California. In addition, Fidonet, a popular traditional bulletin board system (BBS) joins the net.

Dan Lynch organizes the first Interop commercial conference in San Jose for vendors whose TCP/IP products interoperate reliably. Fifty companies make the cut and 5,000 networkers come to see it all running, to see what works, and to learn what doesn't work.

The US Government pronounces its OSI Profile (GOSIP) is to be supported in all products purchased for government use, and states that TCP/IP is an interim solution!

The Morris WORM burrows on the Internet into 6,000 of the 60,000 hosts now on the network. This is the first worm experience and DARPA forms the Computer Emergency Response Team (CERT) to deal with future incidents.

CNRI obtains permission from the Federal Networking Council and from MCI to interconnect the commercial MCI Mail service to the Internet. This broke the barrier to carrying commercial traffic on the Internet backbone. By 1989 MCI Mail, OnTyme, Telemail and CompuServe had all interconnected their commercial e-mail systems to the Internet and, in so doing, interconnected with each other for the first time. This was the start of commercial Internet services in the United States (and possibly the world).

1989: The number of hosts increases from 80,000 in January to 130,000 in July to over 160,000 in November!

Australia, Germany, Israel, Italy, Japan, Mexico, Netherlands, New Zealand and the United Kingdom join the Internet.

Commercial e-mail relays start between MCIMail through CNRI and Compuserve through Ohio State. The Internet Architecture Board reorganizes again reforming the IETF and the IRTF.

Networks speed up. NSFNET T3 (45 Mbps) nodes operate. At Interop 100 Mbps LAN technology, known as FDDI, interoperates among several vendors. The telephone companies start to work on their own wide area packet switching service at higher speeds – calling it SMDS.

Bob Kahn and Vint Cerf at CNRI hold the first Gigabit (1,000 Mbps) Testbed workshops with funding from ARPA and NSF. Over 600 people from a wide range of industry, government, and academia attend to discuss the formation of 6 gigabit testbeds across the country.

The Cray 3, a direct descendant of the Cray line, starting from the CDC 6600, is produced.

In Switzerland at CERN Tim Berners-Lee addresses the issue of the constant change in the currency of information and the turn-over of people on projects. Instead of an hierarchical or keyword organization, Berners-Lee proposes a hypertext system that will run across the Internet on different operating systems. This was the World Wide Web (WWW).

1990: ARPANET formally shuts down. In 20 years, "the net" has grown from four to over 300,000 hosts. Countries connecting in 1990 include Argentina, Austria, Belgium, Brazil, Chile, Greece, India, Ireland, South Korea, Spain, and Switzerland.

Several search tools, such as ARCHIE, Gopher, and WAIS start to appear. Institutions like the National Library of Medicine, Dow Jones, and Dialog are now on line.

More "**worms**" burrow on the net, with as many as 130 reports leading to 12 real ones! This is a further indication of the transition to a wider audience.

1991: The net's dramatic growth continues with NSF lifting any restrictions on commercial use. Interchanges form with popular providers such as UUNET and PSInet. Congress passes the Gore Bill to create the National Research and Education Network, or NREN initiative. In another sign of popularity, privacy becomes an "issue," with proposed solutions such as Pretty Good Privacy (PGP).

The NSFNET backbone upgrades to T3, or 44 Mbps. Total traffic exceeds 1 trillion bytes, or 10 billion packets per month! Over 100 countries are now connected with over 600,000 hosts and nearly 5,000 separate networks.

WAIS's and Gophers help meet the challenge of searching for information throughout this exploding infrastructure of computers.

1992: The Internet becomes such a part of the computing establishment that a professional society forms to guide it on its way. The Internet Society (ISOC), with Vint Cerf and Bob Kahn among its founders, validates the coming of age of internetworking and its pervasive role in the lives of professionals in developed countries. The IAB and its supporting committees become part of ISOC.

The number of networks exceeds 7,500 and the number of computers connected passes 1,000,000. The MBONE for the first time carries audio and video. The challenge to the telephone network's dominance as the basis for communicating between people is seen for the first time; the Internet is no longer just for machines to talk to each other.

During the summer, students at NCSA in University of Illinois at Urbana-Champaign modify Tim Berners-Lee's hypertext proposal. In a few weeks MOSAIC is born within the campus. Larry Smarr shows it to Jim Clark, who founds Netscape as a result.

The WWW bursts into the world and the growth of the Internet explodes like a supernova. What had been doubling each year now doubles in three months. What began as an ARPA experiment has, in the span of just 30 years, become a part of the world's popular culture.

The milestones during this period are: APRANET connects four nodes in 1969; Telnet proposed in 1974; incorporating TCP/IP protocol in Unix system in 1976; client/server model on USENET in 1979; DNS is introduced with its common domains such as .com, .edu, .gov in 1984; TCP/IP interconnected hosts reached 2,000 on the Internet in 1985; NSFNET upgraded to T1 connecting eight countries in 1988; the Morris worm spread the Internet in 1988; more worms burrow on Internet in 1990; the first browser Mosaic came to earth in 1992.

In 30 years, Internet has become a vital part in our daily life. Technology innovation speeded fast, on the other hand, computer and network security emerged as the result of worms and viruses.

1.1.3 Timeline of Computer Security History

The broad concept of computer security happened long before computers were invented. However attacks on computers and networks had not become common until the early 1990s. Now, it becomes not only a serious problem to regular computer users, organizations and government agencies but also a threat to national security.

1965: William D. Mathews from MIT found a vulnerability in a Multics CTSS running on a IBM 7094. This flaw discloses the contents of the password file. The issue occurred when multiple instances of the system text editor were invoked, causing the editor to create temporary files with a constant name. This would inexplicably cause the contents of the system CTSS password file to display to any user logging into the system.

1971: John T. Draper (later nicknamed Captain Crunch), his friend Joe Engressia, and blue box phone phreaking hit the news with an *Esquire* feature story.

1981: The Warelords forms in the United States, founded by Black Bart (cracker of Dung Beetles in 1982) in St. Louis, Missouri, and was composed of many teenage hackers, phreakers, coders, and largely black hat-style underground computer geeks. One of the more notable group members was Tennessee Tuxedo, a young man who was instrumental in developing conference calls via the use of trunk line phreaking via the use of the Novation Apple Cat II that allowed them to share their current hacks, phreaking codes, and new software releases. Other notable members were The Apple Bandit, Krakowicz, and Krac-man. Black Bart was clever at using his nationally known and very popular BBS system in order to promote the latest gaming software. He used that relationship to his advantage, often shipping the original pre-released software to his most trusted code crackers during the beta-testing phase, weeks prior to their public release. The Warelords often collaborated with other piracy groups at the time, such as The Syndicate and The Midwest Pirates Guild and developed an international ring of involved piracy groups that reached as far away as Japan. Long before the movie War Games went into pre-production, The Warelords had successfully infiltrated such corporations and institutions as The White House, Southwestern Bell "Ma Bell" Mainframe Systems, and large corporate providers of voice mail systems.

1990: Operation Sundevil introduced. After a prolonged sting investigation, Secret Service agents swoop down on organizers and prominent members of BBSs in 14 US cities including the Legion of Doom, conducting early-morning raids and arrests. The arrests involve and are aimed at cracking down on credit-card theft and telephone and wire fraud. The result is a breakdown in the hacking community, with

members informing on each other in exchange for immunity. The offices of Steve Jackson Games are also raided, and the role-playing sourcebook GURPS Cyberpunk is confiscated, possibly because the government fears it is a "handbook for computer crime." Legal battles arise that prompt the formation of the Electronic Frontier Foundation, including the trial of Knight Lightning.

Australian federal police tracking Realm members Phoenix, Electron, and Nom are the first in the world to use a remote data intercept to gain evidence for a computer crime prosecution.

1994: Summer: Russian crackers siphon $10 million from Citibank and transfer the money to bank accounts around the world. Vladimir Levin, the 30-year-old ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel. Levin stands trial in the United States and is sentenced to three years in prison. Authorities recover all but $400,000 of the stolen money.

Hackers adapt to emergence of the World Wide Web quickly, moving all their how-to information and hacking programs from the old BBSs to new hacker Web sites.

AOHell is released, a freeware application that allows a burgeoning community of unskilled script kiddies to wreak havoc on America Online. For days, hundreds of thousands of AOL users find their mailboxes flooded with multi-megabyte e-mail bombs and their chat rooms disrupted with spam messages.

1996: Hackers alter Web sites of the United States Department of Justice (August), the CIA (October), and the US Air Force (December).

Canadian hacker group, Brotherhood, breaks into the Canadian Broadcasting Corporation.

The US General Accounting Office reports that hackers attempted to break into Defense Department computer files some 250,000 times in 1995 alone. About 65% of the attempts were successful, according to the report.

The MP3 format gains popularity in the hacker world. Many hackers begin setting up sharing sites via FTP, Hotline, IRC, and Usenet.

1997: A 15-year-old Croatian youth penetrates computers at a US Air Force base in Guam.

June: Eligible Receiver 97 tests the American government's readiness against cyberattacks.

December: Information Security publishes first issue.

First high-profile attacks on Microsoft's Windows NT operating system.

In response to the MP3 popularity, the Recording Industry Association of America begins cracking down on FTPs. The RIAA begins a campaign of lawsuits shutting down many of the owners of these sites including the more popular ripper/distributors The Maxx (Germany, age 14), Chapel976 (USA, age 15), Bulletboy (UK, age 16), Sn4rf (Canada, age 14) and others in their young teens via their ISPs. Their houses are raided and their computers and modems are taken. The RIAA fails to cut off the head of the MP3 beast and within a year and a half, Napster is released.

1998: January: Yahoo! notifies Internet users that anyone visiting its site in recent weeks might have downloaded a logic bomb and worm planted by hackers claiming a "logic bomb" will go off if Kevin Mitnick is not released from prison.

January: Anti-hacker runs during Super Bowl XXXII.

February: The Internet Software Consortium proposes the use of DNSSEC (domain-name system security extensions) to secure DNS servers.

May 19: The seven members of the hacker think tank known as L0pht testifies in front of the US congressional Government Affairs committee on "Weak Computer Security in Government."

June: Information Security publishes its first annual Industry Survey, finding that nearly three-quarters of organizations suffered a security incident in the previous year.

October: "US Attorney General Janet Reno announces National Infrastructure Protection Center."

1999: Software security goes mainstream in the wake of Microsoft's Windows 98 release, 1999 becomes a banner year for security (and hacking). Hundreds of advisories and patches are released in response to newfound (and widely publicized) bugs in Windows and other commercial software products. A host of security software vendors release anti-hacking products for use on home computers.

The Electronic Civil Disobedience project, an online political performance-art group, attacks the Pentagon calling it conceptual art and claiming it to be a protest against the US support of the suppression of rebels in southern Mexico by the Mexican government. ECD uses the FloodNet software to bombard its opponents with access requests.

US President Bill Clinton announces a $1.46 billion initiative to improve government computer security. The plan would establish a network of intrusion detection monitors for certain federal agencies and encourage the private sector to do the same.

January 7: an international coalition of hackers (including CULT OF THE DEAD COW, 2600's staff, Phrack's staff, L0pht, and the Chaos Computer Club) issued a joint statement condemning the LoU's declaration of war. The LoU responded by withdrawing its declaration.

A hacker interviewed by Hilly Rose during the Art Bell Coast-to-Coast Radio Show exposes a plot by Al-Qaida to derail Amtrak trains. This results in ALL trains being forcibly stopped over Y2K as a safety measure.

March: The Melissa worm is released and quickly becomes the most costly malware outbreak to date.

July: CULT OF THE DEAD COW releases Back Orifice 2000 at DEF CON.

August: Kevin Mitnick, "the most wanted man in cyberspace," sentenced to five years, of which over four years had already been spent pre-trial including eight months solitary confinement.

September: Level Seven hacks the US Embassy in China's Web site and places racist, anti-government slogans on embassy site in regards to 1998 US embassy bombings.

September 16: The United States Department of Justice sentences the "Phone Masters."

October: American Express introduces the "Blue" smart card, the industry's first chip-based credit card in the US.

2000: May: The ILOVEYOU worm, also known as VBS/Loveletter and Love Bug worm, is a computer worm written in VBScript. It infected millions of computers worldwide within a few hours of its release. It is considered to be one of the most damaging worms ever. It originated in the Philippines; made by an AMA Computer College student for his thesis.

September: teenage hacker Jonathan James becomes first juvenile to serve jail time for hacking.

2001: Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to Microsoft's Web sites are corrupted.

February: A Dutch cracker releases the Anna Kournikova virus, initiating a wave of viruses that tempts users to open the infected attachment by promising a sexy picture of the Russian tennis star.

April: FBI agents trick two into coming to the US and revealing how they were hacking US banks.

May: Spurred by elevated tensions in Sino-American diplomatic relations, US and Chinese hackers engage in skirmishes of Web defacements that many dub "The Sixth Cyberwar."

July: Russian programmer Dmitry Sklyarov is arrested at the annual Def Con hacker convention. He is the first person criminally charged with violating the Digital Millennium Copyright Act (DMCA).

August: Code Red worm, infects ts.

2002: January: Bill Gates decrees that Microsoft will secure its products and services, and kicks off a massive internal training and quality control campaign.

May: Klez.H, a variant of the worm discovered in November 2001, becomes the biggest malware outbreak in terms of machines infected, but causes little monetary damage.

June: The Bush administration files a bill to create the Department of Homeland Security, which, among other things, will be responsible for protecting the nation's critical IT infrastructure.

August: Researcher Chris Paget publishes a paper describing "shatter attacks," detailing how Windows' unauthenticated messaging system can be used to take over a machine. The paper raises questions about how securable Windows could ever be.

October: The International Information Systems Security Certification Consortium – (ISC)2 – confers its 10,000th CISSP certification.

2003: The hacker group Anonymous was formed.

March: CULT OF THE DEAD COW and Hacktivismo are given permission by the United States Department of Commerce to export software utilizing strong encryption.

December 18: Milford Man pleas guilty to hacking.

2004: March: Myron Tereshchuk is arrested for attempting to extort $17 million from Micropatent.

July: North Korea claims to have trained 500 hackers who successfully crack South Korean, Japanese, and their allies' computer systems.

2005: April 2: Rafael Núñez aka RaFa, a notorious member of the hacking group World of Hell is arrested following his arrival at Miami International Airport for breaking into the Defense Information Systems Agency computer system on June 2001.

September 13: Cameron Lacroix is sentenced to 11 months for gaining access to T-Mobile USA's network and exploiting Paris Hilton's Sidekick.

November 3: Jeanson James Ancheta, whom prosecutors say was a member of the "Botmaster Underground," a group of script kiddies mostly noted for their excessive use of bot attacks and propagating vast amounts of spam, was taken into custody after being lured to FBI offices in Los Angeles.

2006: January: One of the few worms to take after the old form of malware, destruction of data rather than the accumulation of zombie networks to launch attacks from, is discovered. It had various names, including Kama Sutra (used by most media reports), Black Worm, Mywife, Blackmal, Nyxem version D, Kapser, KillAV, Grew and CME-24. The worm would spread through e-mail client address books, and would search for documents and fill them with garbage, instead of deleting them to confuse the user. It would also hit a Web page counter when it took control, allowing the programmer who created it as well as the world to track the progress of the worm. It would replace documents with random garbage on the third of every month. It was hyped by the media but actually affected relatively few computers, and was not a real threat for most users.

February: Direct-to-video film The Net 2.0 is released, as a sequel to The Net, following the same plotline, but with updated technology used in the film, using different characters, and different complications. The director of The Net 2.0, Charles Winkler, is son of Irwin Winkler, the director of The Net.

May: Jeanson James Ancheta receives a 57-month prison sentence, and is ordered to pay damages amounting to $15,000.00 to the Naval Air Warfare Center in China Lake and the Defense Information Systems Agency, for damage done due to distributed denial of service (DDoS) attacks and hacking. Ancheta also had to forfeit his gains to the government, which include $60,000 in cash, a BMW, and computer equipment.

May: Largest Defacement in Web history is performed by the Turkish hacker iSKORPiTX who successfully hacked 21,549 websites in one shot.

July: Robert Moore and Edwin Pena featured on Americas Most Wanted with Kevin Mitnick presenting their case commit the first VOIP crime ever seen in the

USA. Robert Moore served two years in federal prison with a $152,000.00 restitution while Edwin Pena was sentenced to 10 years and a $1 million restitution.

September: Viodentia releases FairUse4WM tool which would remove DRM information off WMA music downloaded from music services such as Yahoo Unlimited, Napster, Rhapsody Music and Urge.

2007: May 17: Estonia recovers from massive denial-of-service attack.

June 13: FBI Operation Bot Roast finds over 1 million botnet victims.

June 21: A spear phishing incident at the Office of the Secretary of Defense steals sensitive US defense information, leading to significant changes in identity and message-source verification at OSD.

August 11: United Nations Web site hacked by Turkish Hacker Kerem125.

October 7: Trend Micro Web site successfully hacked by Turkish hacker Janizary (aka Utku).

November 29: FBI Operation Bot Roast II: 1 million infected PCs, $20 million in losses and eight indictments.

2008: January 17: Project Chanology; Anonymous attacks Scientology Web site servers around the world. Private documents are stolen from Scientology computers and distributed over the Internet.

March 7: Around 20 Chinese hackers claim to have gained access to the world's most sensitive sites, including The Pentagon. They operate from a bare apartment on a Chinese island.

2009: April 4: Conficker worm infiltrated millions of PCs worldwide including many government-level top-security computer networks.

2010: March 24: UN department of safety and security hacked by Turkish hacker DigitALL (1923Turk) Mirror Link.

January 12: Operation Aurora Google publicly reveals that it has been on the receiving end of a "highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google."

June: Stuxnet The Stuxnet worm is found by VirusBlokAda. Stuxnet was unusual in that while it spread via Windows computers, its payload targeted just one specific model and type of SCADA system. It slowly became clear that it was a cyber attack on Iran's nuclear facilities – with most experts believing that Israel was behind it – perhaps with US help.

December 3: The first Malware Conference, MALCON takes place in India. Malware coders are invited to showcase their skills at this annual event and an advanced malware for Symbian OS is released.

2011: The Hacker group Lulz security is formed.

April 17: An "external intrusion" sends the PlayStation Network offline, and compromises personally identifying information (possibly including credit card details) of its 77 million accounts, in what is claimed to be one of the five largest data breaches ever.

The hacker group LulzRaft is formed.

September: Bangladeshi hacker TiGER-M@TE made world record in defacement history by hacking 700,000 Web sites in one shot.

October 16: The YouTube channel of Sesame Street was hacked, streaming pornographic content for about 22 minutes.

November 1: The main phone and Internet networks of the Palestinian territories sustained a hacker attack from multiple locations worldwide.

December 14: Five members of the Norwegian hacker group Noria were arrested, allegedly suspected for hacking into the e-mail account of the terrorist Anders Behring Breivik.

2012: Saudi hacker, 0xOmar, published over 400,000 credit cards online, and threatened Israel with the release 1 million credit cards in the future.

In response to that incident, an Israeli hacker published over 200 Saudi's credit cards online.

January 6: Hacker group The Hacker Encrypters found and reported an open SQLi exploit on Facebook. The results of the exploit have been posted on Pastebin.

January 7: Team Appunity, a group of Norwegians who knew how to use sqli tools developed by others, got arrested for breaking into and publishing the user database of Norway's largest prostitution Web site.

February 8: Foxconn is hacked by rising hacker group, Swagg Security, releasing a massive amount of data including e-mail logins, server logins, and even more alarming – bank account credentials of large companies like Apple and Microsoft. Swagg Security stages the attack just as a Foxconn protest ignites against terrible working conditions.

After 50 years' of computer architecture innovation and 30 years of Internet revolution, we are now in the situation of finding ways to protect the computer systems. Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and many other types of security equipment are common practice but still no one can guarantee that information stored on computers cannot be stolen. This book hopes to address this problem and to discuss solutions to prevent data bleaches on computers.

1.2 John von Neumann Computer Architecture

The Neumann architecture was the first modern design for computers based on the stored program concept (Dumas, 2006). Figure 1.3 shows a block diagram of Neumann architecture. The arithmetic and logic unit is the place where calculations take place. The control unit interprets the instructions and coordinates the operations. Memory is used to store instructions and data as well as intermediate results. Input and output interfaces are used to read data and write results.

Neumann defines a computer as a "very high speed automatic digital computing system, and in particular with its logical control." (Foster and Iberall, 1985)

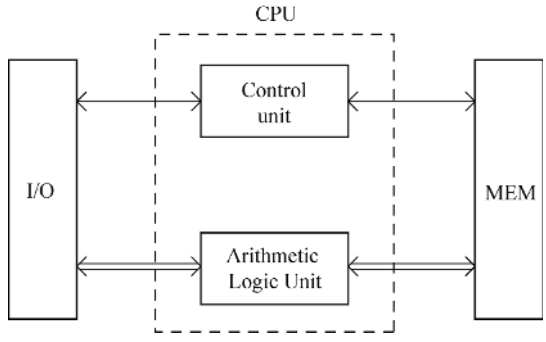

Figure 1.3 Neumann computer architecture

As a computing device, it will have to perform the elementary arithmetic operations most frequently including addition, subtraction, multiplication, and division. It may be extended to include such operations as square roots, logarithmic, and triangulation (sin, cos, arcsin, arccos). This part is the central arithmetical (CA) component which could be considered as central arithmetic and logic unit (ALU).

The logic control device is used to proper sequence its operations more efficiently by a central control (CC) component. A considerable memory is needed to carry out a multiplication or a division and store a series of intermediate results. Various parts of this memory have to perform functions which differ somewhat in their nature and considerably in their purpose. At any rate the total memory constitutes the specific part of a computer system: M.

The three specific parts CA, CC (double C which is now named the central processing unit) and M correspond to the associate neurons in the human nervous system. There are input and output components that are equivalent to the motor or efferent neurons.

In summary, Neumann architecture depicts a computer as a machine with a central processing unit (CPU), internal memory (M) and external storage (S), input/output devices (I/O) and wires that link them together called a bus.

Nowadays, computers still stick to this architecture. When purchasing a computer, people usually consider how fast the CPU or multi-core CPU is, how big the (internal) memory and hard drive are, and how well the I/O is such as the video card, screen size and multimedia features, and so on.

RISC, or reduced instruction set computer, is another type of computer architecture that utilizes a small, highly-optimized set of instructions, rather than a more specialized set of instructions. RISC processors have a CPI (clock per instruction) of one cycle (Shiva, 2000). This is due to the optimization of each instruction on the CPU and a technique called pipelining. Pipelining allows for simultaneous execution of instructions to speed up the execution speed. RISC also uses a large number of registers to prevent large amounts of interaction with memory.

Parallel processing architecture uses multiple processors to form a super computer to solve large problems. The task is often broken into small pieces and distributed across multiple processors or machines, and solved concurrently.

From a security point of view, both RISC architecture and parallel processing architecture still fall into the Neumann architecture category. RISC uses one cycle execution time to improve the efficiency in pipelining. The change is mostly within the processors. The other system components (memory, I/O, storage) are still the same as Neumann's. Parallel processing, on the other hand, contains multiple processors or computers. Each one is a Neumann architecture computer.

1.3 Memory and Storage

As Neumann has described, memory is used to carry out arithmetic operations and store intermediate results. There are two factors to the memory that affect a computer speed the most: the size and the speed. More memory can result in less intermediate results storage and less operation therefore improved computer speed. High speed memory can reduce the delays during each operation. A complex problem requires a tremendous amount of computation. Thus the delay would be significant if a low speed memory is used.

The ideal memory can be characterized as zero or less delay in read and write access, large scale or high density in size, reliable and durable, less expensive and low power. That is why memory is now divided into different categories. Memory closer to CPU is usually faster and more expensive. So it is usually small in capacity. Memory far away from CPU is usually slower and less expensive. So it is usually large in capacity. We often refer to it as storage. USB flash drives and hard drives are examples of external memories or storages.

The read and write property for most memories make them convenient to store data. On the other hand, it also easily altered if a computer is compromised. So memory needs to be defined into regions where program and data are separated. In addition some policies and security measures need to be implemented.

Computer memory is organized into hierarchies centered with the CPU. Registers are the fastest memory. They are specially wired to guarantee the maximum speed. Cache memory is the next fastest memory. The idea behind using cache is to reduce the time for CPU to read/write data directly from the main memory, as this may cause longer delay. Cache memory usually uses static RAM or SRAM, is accessed by blocks and is often divided into two to three levels. Main memory has much larger capacity to store application and data. It usually uses dynamic RAM or DRAM, a type of memory that is cheaper and can be highly integrated, but with a little bit less speed than SRAM.

Hard drives are external memory or storage that has a vast amount of capacity. Solid state drive (SSD) is a new type of storage that acts as a normal hard drive but

without mechanical movements. So they are more reliable and faster. With the advancement of technology, SSDs are becoming cheaper and more affordable.

Virtual memory emerges as a result of applications which need more and more memory to improve performance. Virtual memory by its name is virtual. There is no physical memory associated with it. So virtual memory uses a region of external memory to store programs and data.

Main memory is usually divided into different segments: program, data, data buffers and so on. If a section, for example the data buffer, is extended beyond the limit reserved for that section, then overflow may affect the other segment. If data overflow to the program segment, then programs may execute with unexpected results. If the overflow is set by an attacker, then it may direct the program execution to some preset areas where malicious programs reside, the attacker may take control of the computer system and do even more damage to the computer system. This is called the buffer overflow attack.

1.4 Input/Output and Network Interface

Computer systems typically have several I/O devices. The I/O interface is used to receive data in or write data out with devices such as a keyboard, a mouse, displays, and printers.

Compared with the speed of CPU and memory, a keyboard is a very slow device so an input interface can store data temporally typed from a keyboard and send to memory when reaching the capacity (or buffer size).

A display with animation, however, requires high speed to refresh the screen data. So the interface (video card) needs more speed and more buffer size (or video memory) to accommodate this.

Sometimes, people need to send volume data from input devices to the computer memory without requiring any computation or vice versa. This can be done by using an interface called direct memory access (DMA). The benefit of using a DMA is that data will not go through CPU so a computer can handle other tasks while block data are read in or written out (Randell, 1982).

Computers now are interconnected through network or Internet. Most people check emails every day if not every hour. Vast information can be found on the Internet. So a network interface card (NIC) has become an integral part of a computer system to handle data communication needs.

Computer networks did not exist in Neumann's age so there was no network component on an old computer. People usually consider a network component as essentially belonging to the input and output devices. When we look carefully at the differences between a general I/O and a network component, we can find out that a network by no mean can be considered simply as a general I/O device.

With the widespread use of the Internet in the 1990s, data security has become a problem. Hackers are able to break into computers and servers to steal data, in many

cases sensitive data. The loss caused by the data bleach has reached multiple billion dollars every year and is still on the increase. The damage is beyond money and threatens national security. As a result, network security has become a big challenge in everyday server and computer operations.

I/O devices have slower speed compared to processors. Synchronous communication between them may cause problems. I/O devices will lose data if CPU sends/receives data using processor cycles. On the other hand, according to the I/O device speed, the CPU would have to wait during each I/O operation, thus downgrading the performance. Interrupt is a signal that is used when collaborating communications between high speed processors and low speed I/O devices. When an I/O device has finished handling data it received from the processor, it issues an interrupt request. When CPU receives the request, it saves the current environment, sends/receives data and then resumes the original tasks.

There are different interfaces to connect the processor and the I/O devices. Many recent I/O devices are equipped with the universal series bus (USB). USB unifies the interfaces with its easy to use, plug-and-play connectivity, and hot plug characteristics. In addition, the speed of USB is considerable high so that it can support most I/O devices. The new Super Speed USB 3.0 has the transfer speed of 5 Gb/s.

I/O security is also related to data security. Data stored on hard drives may be exposed to attackers especially insider attackers. Encrypting all data on hard drives is one solution but it may result in performance issues. USB storage devices can be used as bootable devices to start a computer. Unauthorized uses can let attackers steal data on computer systems. In places where data security is a concern, the USB ports should be disabled.

1.5 Single CPU and Multiple CPU Systems

Traditional computers contain one central processing unit. It is like a human brain that controls all activities and remembers all things around it. To solve a problem, an algorithm is programmed and executed as a serial stream in instructions. Only one instruction may execute at a time.

A multiple CPU system on the other hand can process a computation task simultaneously by breaking the problem into independent parts (Hwang, 1993). Each CPU then executes a portion of the problem. Such a procedure is called parallel processing. Parallel processing systems contain multiple CPUs that are interconnected or manufactured together as multi-core processors.

Here is an example of a multiple CPU system compared with a single CPU system. Suppose we want to process a color picture. As we know a color picture consists of three basic colors: red, green and blue (RGB). If we process this picture using a computer with three CPUs, then each CPU can process one color. For a single CPU system, theoretically it would have to take triple time to process this picture, first red, then green, and finally blue.

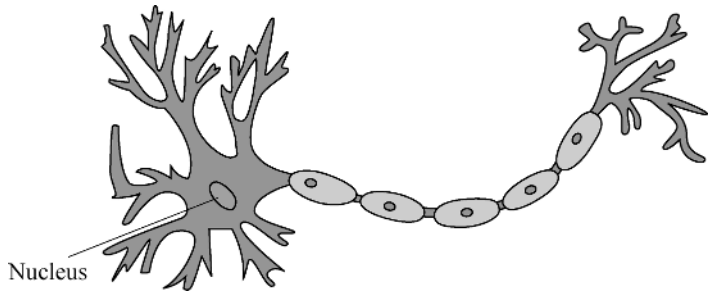

Figure 1.4 Structure of a typical neuron

People often refer to CPU as the "brain" of a computer system. People in some parts of the world think of a computer as an "electronic brain." For a multiple CPU computer system, how does such a match correspond to this image?

If you look inside the brain, there are about 100 billion (10^{11}) neurons. A neuron is a special type of cell that has a nucleus which contains genes and acts like the brain of the cell. It has electrical excitability and the presence of synapses used to transmit signals to other cells. Figure 1.4 shows the structure of a typical neuron.

There is a trend to add more CPUs into a computer. It by no means indicates there will be more "brains" in an identity (here is a computer). Instead some people consider CPUs in parallel processing or multicore computers as "neurons." A parallel processing computer has many CPUs, local memory, and interconnection networks. So it does function like a neuron that contains synapses used to transmit and receive signals between neurons. This may be another explanation for why no matter how many CPUs a computer has, its speed is no match with the human brain because no computer will contain a million CPUs, not to mention the 100 billion neurons in a human brain.

Processors were originally developed with only one core. More and more computers use multi-core processors where each core is acting like an independent processor. The architecture of multi-core processors can be organized as each core contains a CPU and level 1 cache. A bus interface connects all cores and also provides a level 2 cache. All cores and interfaces are integrated on one circuit (one die).

More advanced parallel processing computer systems use multiple processors or an array of processors to form a super computer. The processors can be at a centralized location or they can be at distributed locations.

In corporate businesses, more companies and organizations use services provided for them instead of buying a number of powerful computers (servers). This leads to the cloud computing concept. In a cloud computing model, some companies build the cloud which contains applications, platforms, and infrastructure. Other companies or organizations acting as users use these infrastructures, software and platforms

as services. Since different organizations may share the same cloud, data separation and security are a common concern for running critical applications that contain sensitive data on a cloud.

On the other hand, thin clients also have the momentum as the client is cheaper, consumes much less energy therefore is more "green," and is easy to manage. Thin clients use computation power of a remote computer. The technology is perfect for situations where high speed network is available and animation is not the main concern.

Distributed computing has tremendous power to accomplish jobs which otherwise would not be performed with traditional computers. Pharmaceutical companies use hundreds of thousands of computers distributed across the country to simulate clinical tests. It can greatly shorten the time for a new drugs test. Sophisticated computer hackers can also benefit from using the distributed computing platform. They are able to shut down VISA/Mastercard company's websites and other government websites. They launched so called a distributed denial of service attack, or DDoS attack.

In a typical DDoS attack, the army of the attacker consists of master zombies and slave zombies. The hosts of both categories are compromised machines that have arisen during the scanning process and are infected by malicious code. The attacker coordinates and orders master zombies and they, in turn, coordinate and trigger slave zombies. More specifically, the attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking. Then, master zombies, through those processes, send attack commands to slave zombies, ordering them to mount a DDoS attack against the victim. In that way, the agent machines (slave zombies) begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources. Figure 1.5 shows this kind of DDoS attack.

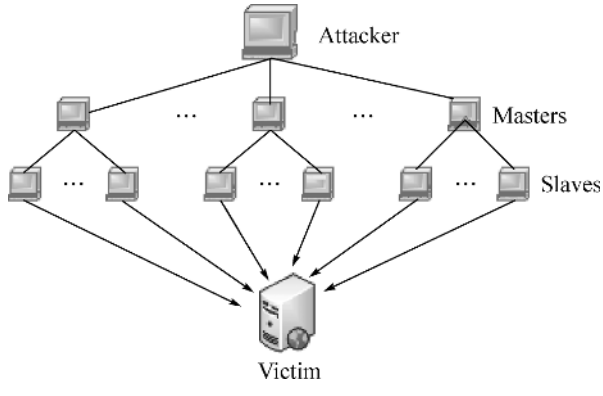

Figure 1.5 A DDoS attack

1.6 Overview of Computer Security

Computer security relies on confidentiality, integrity, and availability. A more comprehensive description includes:

- Authentication
- Authorization
- Confidentiality
- Integrity
- Availability
- Accountability
- Non-repudiation.

Certified information systems security professional (CISSP) classifies information security into ten domains:

- Access Control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations and Compliance
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security.

1.6.1 Confidentiality

From an information security point of view, confidentiality is the concealment of information or resources. From a computer architecture perspective, confidentiality is to design a computer system that is capable of protecting data and preventing intruders from stealing data in computer systems.

Access control mechanisms support confidentiality. A software solution to enforce access control mechanism is cryptography, which encrypts data to make it incomprehensible. A hardware solution is physical separation. Total physical separation is impractical so in many cases we use a hybrid method which is partial physical separation plus (software) access control polices.

Below are two examples that further describe the concept of confidentiality:

Example 1: A company named GEE does not want competitors to be able to see exactly how many or which equipment its clients happen to be ordering from the

company, because that may give them competitive information. So GEE use the secure protocol to encrypt all the communication between its clients and the Web site. (More examples on this case will follow.)

Example 2: A newly proposed computer model enables a computer operator (owner) to control what data can go in and go out. Nobody can get data from this computer system without the permission of the computer operator. In this way, the confidentiality is guaranteed. Interested readers can read Chapter 10 for a detailed technical description about how to design and implement such a secure computer system.

Information hiding is another important aspect of confidentiality. For example, a program can encrypt a secret message into a picture. Only people with the program (or key) can reveal the secret. Without the key, people can only view it as a normal image. An example of such an encryption application programmed by the book author can be downloaded from www.wiley.com/go/wang/comp_arch.

1.6.2 Integrity

Integrity refers to the trustworthiness of data. There are two aspects: data in motion and data at rest. Data in motion usually refers to the origin of the data. Authentication is a way to assure data integrity of this kind. Data at rest means the content of the information itself. When data are stored on a computer, they need to be protected and non-altered.

Here is the example that follows the earlier example described in Section 1.6.1. Suppose that a client named Alice wants to order ten equipments from GEE, but an attacker wants to alter her order to zero equipment. If the attacker succeeds then the client may eventually get frustrated with GEE and might decide to go to a competitor.

1.6.3 Availability

Availability refers to the ability to use the information or resources desired. For enterprise applications running on a server, availability is critical to the success of the business. Attempts to block availability, called denial of service (DoS) attacks, can be difficult to detect. A distributed DoS (DDoS) attack may be even harder to identify.

When designing a secured computer system, there is a tradeoff between availability and confidentiality. We understand that both are important but for a server, availability cannot be sacrificed. While for a personal computer, we may consider sacrificing the availability a little bit to enhance the confidentiality and integrity. For example many people would agree to sacrifice a millisecond (1/1,000 second) to ensure their data will never be stolen.

1.6.4 Threats

A threat is a potential violation of security. The actions that might occur are called attacks. Those who execute such actions are called attackers or hackers. Here are some common threats:

- Snooping: The unauthorized interception of data, such as wiretapping.
- Alteration: An unauthorized change of data, such as man-in-the-middle attack.
- Spoofing: An impersonation of an entity by another.
- Phishing: An e-mail scam that attempts to acquire sensitive information.
- Delay or denial of service: An inhibition of a service.

Computer security is to study, to detect, to prevent threats and to recover from threats. For detection, applications include intrusion detection systems (IDS) and firewalls on the network or installed on a computer. Detection is like building a dam or levee to prevent flood. It is passive and has limited protection.

"Computer architecture and security" aims to study how to design a secure computer system that can **prevent** threats and attacks. In other words, the goal of a secured computer system should be to become immune from attacks.

For recovery, most organizations have a disaster recovery plan, a part of the security policy. In the event of security being bleached, the plan is to help reduce the loss of data and shorten the mean time between failures (MTBF).

1.6.5 Firewalls

Firewalls are software or hardware implementations of a series of algorithms that detect and filter the transmission of information and data (usually divided into small packets). A request to access local resources from outside the firewall can be either granted or denied depending on the policies preset. On the other hand, a request to access local or remote resources can also be granted or denied. Correctly configured firewalls can protect computers or local area networks while still allowing legitimate packets to go through. Sometimes, it is hard to tell whether the communication is an attack string or real data. So tightly configured firewall may block legitimate traffic and is called **false positive**. Loosely configured firewalls, on the other hand, may let the attack string pass through without being detected, and is called **false negative**. This may cause severe damage to the computer system. In our daily life these principles are also very useful. Remember the DC Metro train crash in June 22, 2009. If the metrorail system had a policy to stop any trains in the event of any false alarms, the accident would not have happened.

Firewalls are used to block attacks just like levees are used to block flooded rivers. No matter how robust the levee system is, failure may still happen. Hurricane Katrina in New Orleans is a lesson in this. Similarly, firewalls can only have limited

protection for computer systems. Attackers may find vulnerabilities in firewall algorithms and bypass the firewall to gain access to the computer systems. Computer security should not only rely on passive detecting techniques, it should expand its scope to work actively to prevent attacks. The invention discussed in Chapter 10 is such a preventing technique.

1.6.6 Hacking and Attacks

Hacking means finding out weaknesses in an established system and exploiting them. A computer hacker is a person who finds out weaknesses in a computer and exploits it. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge (Hacker, 2012). The subculture that has evolved around hackers is often referred to as the computer underground but it is now an open community.

A **white hat** hacker breaks security for non-malicious reasons, for instance testing their own security system. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. Often, this type of "white hat" hacker is called an ethical hacker.

A **black hat** hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain. Black hat hackers are the epitome of all that the public fears in a computer criminal. They break into secure networks to destroy data or make the network unusable for those who are authorized to use it. The way black hat hackers choose the networks that they are going to break into is by a process that can be broken down into two parts: targeting and research and information gathering.

Bots are automated software tools, some freeware, available for use by any type of hacker.

An attack is to compromise a computer system. A typical approach in an attack on an Internet-connected system is:

1. *Network enumeration*. Discovering information about the intended target.
2. *Vulnerability analysis*. Identifying potential ways of attack.
3. *Exploitation*. Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

Here is a list of attacking techniques often used by both black hat attackers and white hat attackers:

- Vulnerability scanner: A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or

available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number.
- Password cracking: Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.
- Packet sniffer: A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.
- Spoofing attack (Phishing): A spoofing attack involves one program, system, or Web site successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.
- Rootkit: A rootkit is designed to conceal the compromise of a computer's security, and can represent any set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.
- Social engineering: When a hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique is to contact the system administrator and play the role of a user who cannot get access to his or her system. Hackers who use this technique have to be quite savvy and choose the words they use carefully, in order to trick the system administrator into giving them information. In some cases only an employed help desk user will answer the phone and they are generally easy to trick. Another typical hacker approach is for the hacker to act like a very angry supervisor and when his/her authority is questioned they will threaten the help desk user with their job. Social Engineering is so effective because users are the most vulnerable part of an organization. All the security devices and programs in the world won't keep an organization safe if an employee gives away a password. Black Hat Hackers take advantage of this fact. Social Engineering can also be broken down into four sub-groups. These are intimidation, helpfulness, technical, and name-dropping.
- Trojan horses: A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder inside.)
- Viruses: A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus

behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

- Worms: Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm," using them both to describe any self-propagating program.
- Key loggers: A key logger is a tool designed to record ("log") every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a point of sale and data collected by the key logger could be used for catching employee fraud.

1.7 Security Problems in Neumann Architecture

In Neumann architecture, memory, storage and I/O are connected directly to CPU. People consider the connections as a path or highway for the data to go through. On the other hand, it functions like a vehicle to carry information between the main components of a computer system. Technically we name it a bus.

A "system bus" representation of the Neumann model is shown in Figure 1.6. This is just another view of the Neumann model, with the introduction of the concept of DMA. DMA enables data exchange directly between memory and I/O that otherwise cannot be done with the initial Neumann model.

Since the 1990s, computer networks especially the Internet has been widespread around the world. Computers are no longer only being used to compute as a stand alone machine. The feature of information exchange through a network becomes a

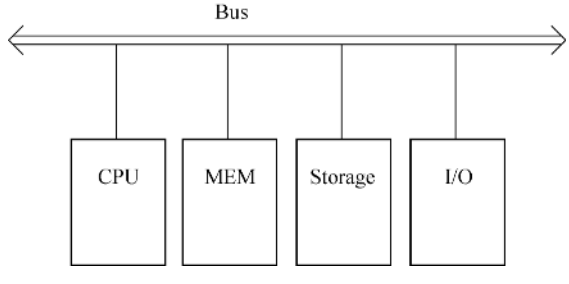

Figure 1.6 A "system bus" representation of the Neumann model. It is equivalent to Figure 1.3 with the introduction of DMA

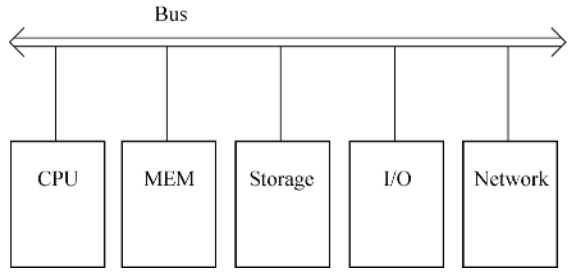

Figure 1.7 Updated Neumann computer architecture model with network interface added and separated from the general I/O devices

vital component in today's computers. Unfortunately John Neumann was not able to foresee this change.

One can argue that we can consider that a network is part of input/output devices which are already included in the Neumann model. However, the network interface is so important that it is not appropriate to classify it as a general I/O device. Furthermore, an I/O device in the Neumann model refers to those devices such as a keyboard, a display, and a printer, and so on, which are used for direct interacting with the computers. Now, the way people use a computer is considerably different to that of 60 years ago. So an update of Neumann's computer architecture model is necessary to reflect this change.

Figure 1.6 shows the modified Neumann model. In Figure 1.7, a network unit (interface) is added to the bus of a computer system. The I/O unit only deals with input and output devices such as keyboard, mouse, and display, and so on. The network interface is responsible for communicating with other computers and devices over the Internet. The separation of network unit from the general I/O devices offers great advantages.

The Neumann model is so dominant that no one has ever challenged it since its birth in 1945. However, if we look into the Neumann model from a security perspective, we could find out that it does have some potential problems.

In the Neumann model, CPUs, Memory, I/O, external storage are all connected to one single bus that includes control bus, data bus, and address bus. Once intruders break into the system from any network location, they can totally take over the computer system and do whatever they want.

For the Neumann model, the concept of CPU is a centralized control and arithmetic unit. Even though nowadays a computer with multiprocessors is very common, those processors are merely coordinated together by software to perform one task or a series of tasks. In other words, they share the same system bus. Intruders can still take over the whole system once they break into the system from any network port.

To solve this problem, numerous people have proposed different methods from securing CPU and memory to securing network interfaces by applying firewalls and

intrusion detection systems. However, those solutions have not solved the information security problems completely due to the limitation of the computer architecture they used. The authors of this book have found out that there is a problem that exists in John von Neumann's computer architecture model – the foundation of modern computer architecture. If this problem is not solved, information stored on a computer will hardly be secure. As a result, a modified Neumann architecture that is capable of securing data stored on computer systems is proposed. More information about the new secured architecture will be discussed in Chapter 10.

1.8 Summary

A computer is composed of hardware, software, network, and data. People have different views about a computer system. The level of abstraction from a computer designer and a general user is different.

Computer architecture is to study how to design computer systems. *Computer Architecture and Security* will teach you how to design secured computer systems. Moreover, this book explains how to secure computer architecture as a whole so that modern computers can be built on new architecture free of data breaches.

The Neumann architecture was the first modern design for computers based on the stored program concept. It is composed of an arithmetic and logic unit (ALU), a control unit (CU), memory (M), storage (S), and input/output (I/O) devices. With the introduction of Internet, a network interface card (NIC) has become an integral part of a computer system.

Computer history reveals invention and innovation from the early days followed by rapid network and Internet development. As technologies for both computers and networks are still growing, concerns about computer and network security are also increasing.

Computer security is to study confidentiality, integrity, and availability of a computer system. The Neumann system uses single bus architecture therefore it is vulnerable to intruder attacks.

Modified Neumann architecture separates network from the other computer components. Experiments and tests have proved that it is capable of securing data stored on a computer system.

Exercises

1.1 Describe the main components of a modern computer system.

1.2 Why is a network interface different to general I/O devices?

1.3 Traditionally, a user's view of a computer system is like an onion. Explain why this concept is outdated and draw a new diagram based on the concept proposed in this book.

1.4 Computer firewalls are used to protect computer from data loss. Why firewalls can not guarantee data security?

1.5 What is a computer bus? Which types of data are carried on a computer bus?

1.6 What are the main advantages of Neumann architecture compared with those of earlier computing devices?

1.7 Draw a diagram of Neumann architecture and a single-bus diagram of Neumann architecture.

1.8 Why is assembly language called low-level language?

1.9 Virtualization sometimes is called "computers on a computer." Describe how this works?

1.10 What are the differences between memory and storage?

1.11 Discover the NIC(s) on your computer? Is it wired or wireless?

1.12 Why is Neumann architecture still considered the architecture for multiple CPU computers or multicore computers.

1.13 Provide an example for each of the following security terms: authentication, authorization, confidentially, integrity, and availability.

1.14 What is cryptography? If you want to send a secret message to your friend using a computer, what is the best way to do it?

1.15 What does the term DoS attack stand for?

1.16 List some common threats to a computer system and network.

1.17 What are the problems that exist in Neumann architecture? How can those problems be addressed?

1.18 Suppose Alice is an employee of a hospital called FX Hospital, and her job responsibility is to order medical equipment for the hospital from a company called GEE. GEE has a Web site that Alice to procure medical equipment for her hospital. Answer the following questions.

(1) Alice has to log into GEE and give that Web site her username and password through SSL protocol so that GEE knows that it is Alice. This is called _____.

Authorization, authentication, confidentiality, integrity

(2) If Alice tries to order equipment from GEE, the website will allow it, but if Bob attempts to order equipment, the order will be rejected. The website does this by conducting _____ check.

Security, accountability, authentication, authorization

(3) The SSL protocol encrypts all the communication between Alice and the GEE Web site with an algorithm such as Triple DEC to make sure of the _____ of the information.

Integrity, availability, confidentiality, security

(4) The SSL protocol uses message authentication codes in the messages that are sent between Alice and the Web site to make sure that no competitor or other malicious party can tamper with the data. This is to ensure the data's _____.

Confidentiality, integrity, accountability, non-repudiation

(5) GEE have a competitor that launches a DoS attack against the site in order that Alice will stop buying from GEE and instead come to their competing site. This affects the GEE website's _____.

Confidentiality, deny of service, integrity, availability

(6) Every time Alice places an order from the GEE website, it produces a log entry so that Alice cannot later claim to have not ordered the equipment. This is to ensure the _____.

Integrity, authentication, authorization, accountability

(7) If the web browser and website run a _____ protocol, it is then possible for Alice to prove to a third party that she only ordered, say, 10 equipments, and not the 12 that GEE may claim she ordered.

TCP/IP, non-repudiation, repudiation, multicast

References

Computer history (2012) Computer history museum. Retrieved March 8 2010 at www.computerhistory.org

Dumas, J.D. (2006) *Computer Architecture: Fundamentals and Principles of Computer Design*, Taylor & Francis.

Foster, C.C. and Iberall, T. (1985) *Computer Architecture*, 3rd edn, Wan Nostrand Reinhold Company, New York.

Hacker (computer security) (2012) Wikipedia. Retrieved February 2 2012 at http://en.wikipedia.org/wiki/Hacker_(computer_security).

Hwang, K. (1993) *Advanced Computer Architecture: Parallelism, Scalability, Programmability*, McGraw-Hill, Inc.

Randell, B. (ed.) (1982) *The Designs of Digital Computers*, Springer-Verlag.

Shiva, S.G. (2000) *Computer Design and Architecture*, 3rd edn, Marcel Dekker, Inc., New York.