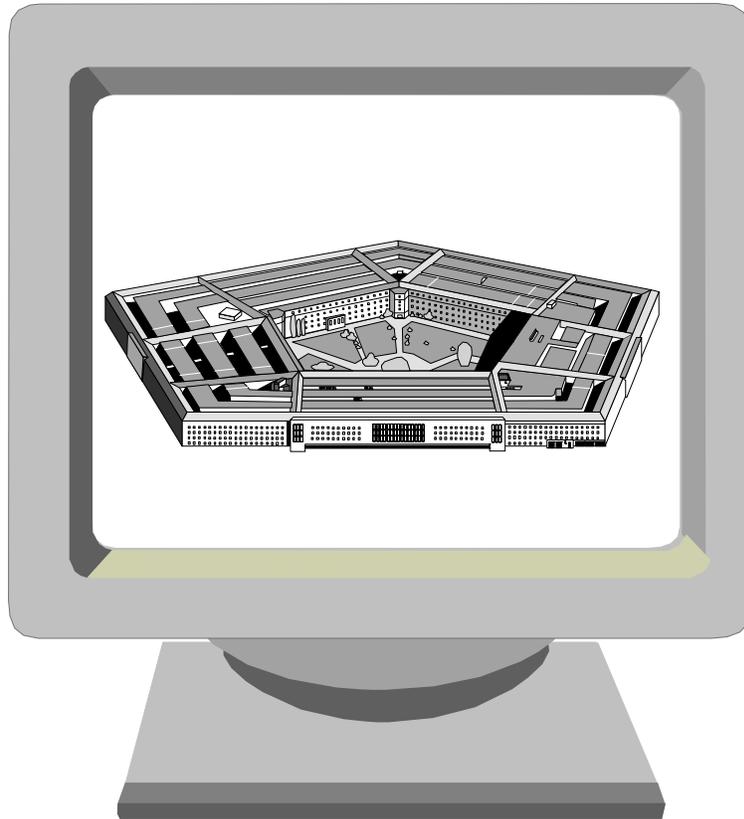




Information System Security Basics



DEFENSE SECURITY SERVICE
ACADEMY
938 ELKRIDGE LANDING ROAD
LINTHICUM, MARYLAND 21090

Version 1.0

TABLE OF CONTENTS

INTRODUCTION	3
ASK FOR ASSISTANCE	3
HARDWARE/SOFTWARE/FIRMWARE	4
BITS AND BYTES	5
BOOTING THE COMPUTER	5
LANGUAGES	6
OPERATING SYSTEM (OS)	7
TYPES OF COMPUTERS	8
SIZES OF COMPUTERS	9
CATEGORIES OF MICROCOMPUTERS	10
BASIC COMPUTING COMPONENTS	12
THE CENTRAL PROCESSING UNIT	12
STATES OF MEMORY	14
SIZE OF MEMORY	14
PERIPHERAL DEVICES	15
TYPES OF MEMORY	15
STORAGE DEVICES	17
INPUT DEVICES	18
OUTPUT DEVICES	18
INPUT/OUTPUT (I/O) DEVICES	19
TELECOMMUNICATIONS	19
DISCONNECT METHODS	20
TEMPORARY FILES	21
PRINTER TECHNOLOGIES	21
MODULATOR/DEMULATOR (MODEM)	23
FAULT-TOLERANT SYSTEM(S)	24
MODIFICATIONS MAY LEAD TO PROBLEMS	24
SECURITY IN REVIEW	26
RESOURCES AVAILABLE TO YOU	27
CONCLUSION	28
INDEX	29

INTRODUCTION

The purpose of this booklet is to introduce you to terminology, technology and basic security concerns associated with information systems. After reading this booklet, you should be able to **define basic computer terms** which are commonly used in the computer industry as well as the Department of Defense (DOD); **describe types of hardware, software, and peripheral devices**; and **discuss security implications** that result from these technologies.

Whether you are reading this booklet as a prerequisite to a DSS ACADEMY course or just because you want to learn more about computer security, we welcome your comments and questions. The last page of this booklet identifies a point of contact for your assistance. *If this booklet is a prerequisite for a course, you must pass the exam with a 75% score prior to enrolling in the requisite course (i.e. NISPOM Chap 8 Requirements for Industry).*

ASK FOR ASSISTANCE

One of the biggest problems encountered by novice computer users and system security officers is not being able to communicate with technically adept computer systems personnel. As the person tasked with establishing and maintaining system security, you must understand how technologies and configurations affect this responsibility. Whenever one of your technical representatives discusses a term or uses vocabulary that you are unfamiliar with say, "Please explain what you mean by _____." Insist that they talk to you in terms that you can understand. If they state that they will be using a certain type of storage media, ask questions about this media . . . what is it, what does it look like, how is it to be used and by whom? Ask all these questions and be sure to get the answers that you require. Any technical person (techie) should be able to describe (in layman's terms) exactly what the technology is, how it works, and how it affects security.



At times you may find that we in the DOD do not necessarily use the data processing community's definition for certain terms. For example, the term **remote** according to our DOD definition refers to any device outside of the physical control of the computer facility (CF) or the system administrator's line of sight. The same term defined by the data processing community refers to a device which communicates (via network or modem) to the CF. This device may be situated within the CF but still be a remote!

HARDWARE/SOFTWARE/FIRMWARE

The physical equipment or any of the machinery that makes up the computer system is known as **hardware**. This term specifically refers to the mechanical devices, nuts, bolts, wiring and the circuitry that comprise a computer. If you bump into it, it's hardware!

In a computer system, all programs (structured instructions) connected with the operation of the computer are referred to as **software**. Software is just as important, if not more important, than the hardware (the computer system). Without software, the computer is nothing more than an expensive door stop. Once a software program is loaded into the computer's memory and the processing is initiated, the pre-programmed instructions are carried out or "executed" one after another, often without human intervention. When we think about software, we normally think about programs such as the Operating System and applications like, spreadsheets, word processing, data base management systems, telecommunications software, and the like.

Firmware is a combination of both hardware and software. It is a category of memory chips that hold their content without electrical power. An example is pre-programmed code placed in a 'chip memory' device for permanent storage on the system (see Read Only Memory). These devices are sometimes installed by computer manufacturers to conduct diagnostic checks of their systems' hardware. Firmware often provides the first computer instructions when a computer is turned on.

BITS AND BYTES



Bit stands for **binary digit**. A bit can be in only one of two states. These states are variously referred to as “on” or “off,” “1” or “0,” “+” or “-,” “true” or “false.” The important point is that it can be in only one of two possible states. Eight of these bits strung together create what is called a **byte**. A byte typically represents a character, either alpha (A, B, C,...) or numeric (1, 2, 3,...). This is the normal form in which information is sent to and from the computer. The term byte is also used as a gauge to measure computer performance or power. You've probably heard of a computer being described in the following fashion: "It has 256 MB of memory and a 80 GB fixed disk." This means that the computer has the capacity to store 256 Megabytes (MB) or 256 x (1024 X 1024 characters) of information in its memory device (usually Random Access Memory, or RAM). The fixed disk capacity was measured in gigabytes (GB) which equates to a billion bytes (or characters) of information that can be stored on its fixed storage device.



BOOTING THE COMPUTER

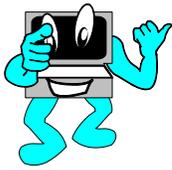
Booting the computer refers to what happens as a computer system initializes (starts), normally after applying power. The term comes from "bootstrap". Bootstraps help you get your boots on. Similarly, booting the computer helps it get its first instructions. The computer **Basic Input Output System (BIOS)**, which is firmware, goes through its built-in diagnostics (self-tests), establishes communications with the various hardware devices and a number of other chores, then turns control of the system over to the operating system (the control program). There are two types of boots: a cold boot (initial application of power) and a warm boot (restarting the computer without turning off the power).

The BIOS, an essential set of routines in a PC, is stored on a chip and provides an interface between the operating system and the hardware. The BIOS supports all peripheral (see Peripheral Devices) technologies and internal services such as the realtime clock (time and date). BIOS not only “glues” the hardware together and does diagnostics, but it can also provide some security for the system. The BIOS has passwording capability, it can be set so that you must enter a password in order to allow the system to boot.

A second password, sometimes called the supervisory password, gives the capability to set a password to protect the BIOS so the settings can't be changed by a normal user. These passwords can be deleted if the user can gain access to the inside of the CPU. Removal of the battery providing power to the BIOS will delete the passwords, as will the moving of a jumper which may be on the computer's motherboard. A jumper is the simplest form of an on/off switch. It is a tiny, plastic-covered metal block, which is pushed onto two pins to close that circuit.

A **warm boot**, such as on an IBM personal computer (PC) or compatible, is normally accomplished by simultaneously pressing the "Ctrl", "Alt" and "Del" keys on the keyboard. These actions do not necessarily remove or purge information which was stored in the system's memory.

A **cold boot** occurs when power is restored to a computer system after power is switched off or a power cord is pulled from its power source. If the system's memory is volatile, all information in the system's memory is lost when the power is removed and therefore not accessible after a cold boot. Sometimes the computer's "reset" switch can also be used to simulate a "cold boot," but this may or may not remove any data from the volatile (usually RAM) memory.



From a security standpoint, a cold boot (turn power off and then on) is preferable to a warm boot. Neither a warm boot nor a "reset" is guaranteed to "zero out" (clear) all of the memory.

LANGUAGES

Quite a comical scene was played out in "Star Trek 4 - The Movie" when a character named "Scotty" sat down at a 20th century computer and tried to issue voice instructions to it. This reminds us how today's most commonly used computers do not yet communicate with us in this manner. While the technology does exist, it is not universal. So for now we have to be satisfied with using devices such as keyboards, mice, digitizer tablets, scanners, etc.

Computers do not understand our language. That is why the computer software industry is such a booming business. If we want the computer to

do something for us, we must rely on the instructions that someone has programmed into its software. The computer only understands two things: 0's and 1's. To issue instructions to the computer in this language, known as **machine language**, a programmer has to know the language and spend time writing and debugging (fixing) long lines of program code. These 0's and 1's allow us to tell the computer what to do, how to do it, and what to store as data. Machine language is also known as **low level language**.

High level languages allow us to prepare program code and communicate with computers in a way that is more user friendly. Instead of a programmer issuing a string of 0's and 1's to tell the computer to print, the programmer might issue a simple "print" instruction. Examples of high level languages are Pascal, ADA, Visual Basic, C, C++, Perl, Python, etc. These high level languages are extremely powerful and, with a little training, quite easy to use.

At some point, the programmer has to convert high-level language (Human readable instructions) into low-level language (machine language) so that the computer can understand it. This is called **compiling**. The security implication of this is that once sensitive information is put into a system (such as programming it to do automated tests or work on an embedded weapons system) and the program has been compiled (converted into 0's and 1's), it normally does not lose its sensitivity. The information is still sensitive. It's in another form, but it is still sensitive information. If a program can be compiled, it may be decompiled.

OPERATING SYSTEM (OS)

A program called an **operating system** or **OS** is the master control program that runs the computer. It is one of the first programs loaded when the computer is turned on, and its main part (called the "kernel") resides in memory at all times. The OS does several things. The OS sets the standards for all application programs that run in the computer. It detects errors associated with the system, software, and/or hardware; and it allocates resources such as printers and communications interfaces such as modems and network interfaces (devices that communicate with other computers). Most operating systems (MVS, VMS, UNIX, Linux, NetWare, Windows

9X, Windows NT, 2000, XP, MacOS) used on computer systems, including PCs, include telecommunications and networking capabilities.

The OS also schedules and prioritizes jobs such as batch (group) print jobs and processing. By giving the computer certain instructions, the operator may change the priorities of these jobs. On most computers today, you will find that security enhancements are part of the OS.

For Operating Systems like Windows 95, 98, ME or early Apple programs there are no security capabilities, and a separate product must usually be purchased to secure the system. Others like Windows NT, 2000, XP and Server 2003, UNIX, Linux, and recent MacOS operating systems have various amounts of security features as part of the OS.

You communicate with the operating system in one of two ways: Command Line Interface (CLI) or Graphical User Interface (GUI). Some PC CLI commands or functions are: FORMAT, DELETE, ERASE, COPY, RENAME. As you can see, these instructions or commands are quite easy to understand, since they are descriptive of the things they do. The functions for other commands, such as ATTRIBUTE, may not be as evident as one would wish, and UNIX/Linux commands can be very hard to decipher, since they tend to be very cryptic.

TYPES OF COMPUTERS

There are two types of computers: general purpose and special purpose. Most systems in use today are **general purpose** in nature. This means that they are designed to be used in performing a variety of functions. For example, a computer system in a large company might be used for payroll, accounting, and inventory control. **Special purpose** computers are task-oriented and may be used for one specific function such as to monitor the toxicity of vapors in a chemical production area or to analyze blood in a hospital, or for various military purposes. Many service stations use special purpose computers to diagnose car problems and identify adjustments that must be made to engines, exhaust systems, etc.

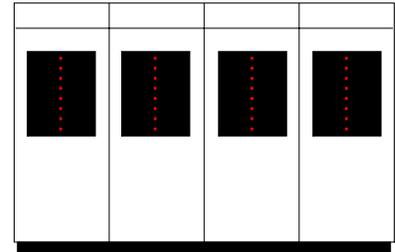


SIZES OF COMPUTERS

There are three general sizes of computers: Micro, Midrange (Minicomputer) and Mainframe. The **microcomputer** generally refers to a Windows PC or Macintosh, but it can refer to any kind of small computer. When the term was first introduced in the late 1970s, it meant a computer with a single microprocessor chip as its CPU (see Central Processing Unit), namely, the personal computer. Today, the CPU in every computer is a microprocessor, and the terms "desktop



computer," "laptop computer" and "PC" have mostly replaced microcomputer and personal computer. The microcomputer is normally designed to be used by one person at a time. It can usually support a small number of devices, such as a printer, a plotter, and/or a scanner. Some microcomputers can also be used as servers. A server is an "upgraded" microcomputer. It is utilized as a hub or host for a centralized network and can be used by several persons. A **minicomputer** was an earlier medium-scale, centralized computer that functioned as a multiuser system for up to several hundred users. The single user minicomputer evolved into a centralized system with dumb terminals for departmental use. During the 1980s and early 1990s, most centralized minicomputers migrated from their dumb terminal architecture into servers for PC networks. The terms "**midrange computer**" and "server" replaced the minicomputer designation. Midrange computers encompass a very broad range and reside in capacity between high-end PCs and mainframes. Most midrange computers today function as servers in a network. It supports several users at a time and numerous peripherals. A peripheral is anything that is not part of the central processing unit (CPU). The differences between midrange and microcomputers are cost (midrange are more expensive), memory and storage capacity (midrange computers have more), and processing speed (midrange are faster due to more sophisticated or multiple processors). Now let's move up to the **mainframe computer**. A mainframe computer is a large computer. In the mid-1960s, all computers were called mainframes, since the term referred to the main CPU cabinet. Today, it refers to a large computer system. Large mainframes use smaller computers as front end processors that connect to the communications



networks. The differences between the midrange and the mainframe are, again, cost, the amount of storage, and the speed and number of processors. Don't be overwhelmed by the size of the computer system - they all function similarly. If you understand the concepts of the microcomputer, you have the knowledge needed to successfully manage the security responsibilities of a large-scale system.

CATEGORIES OF MICROCOMPUTERS

Now, let's identify several different categories of microcomputers. Among these are portables, namely, laptops, notebooks, and palmtops. **Portable computers** are small and can be carried from point to point. When we think of transportable computers, we think of what we first called a portable computer even though its weight and bulky devices actually made it a **luggable computer**. Today, any laptop that weighs more than 10 pounds could be called a luggable. Then came the **laptop computers**. These are called laptop computers because they easily fit on your lap. A laptop computer is a portable computer that has a flat LCD screen and usually weighs less than eight pounds. Often called just a "laptop," it uses batteries for mobile use and AC power for charging the batteries and desktop use. Today's high-end laptops provide all the capabilities of most desktop computers. Then came the **notebook computers**. A Notebook computer is a laptop computer that weighs from approximately five to seven pounds. A notebook that weighs under five pounds is usually called a "subnotebook." Again, one loses very little functionality. Today's notebook computers have as much memory and storage as their desktop counterparts. There are also **tablet PCs** that combine the power of a notebook and compactness of a subnotebook with the added functionality of handwriting recognition.

Even smaller than notebook computers and tablet PCs are **Palmtop computers** and **Personal Digital Assistants (PDAs)**. Palmtops are computers small enough to hold in one hand and operate with the other. Palmtops may have specialized keyboards or keypads for data entry applications or have small keyboards. PDAs are even smaller computers that are generally pen based and use a stylus to tap selections on menus and to enter printed characters. Their shortcomings include limited memory capacity and storage device size when compared to a laptop. The Palmtop keyboards are also difficult for individuals with large hands (and fingers) to

operate. One security concern for these types of computers (as well as some others) is that any classified information stored on these computers might not be removed before they are released from secure or controlled spaces. Another concern is that wireless ports such as Infrared (IR) or Radio Frequency (RF) might be inadvertently transmitting classified information, or that they may be used by uncleared people to access the IR or RF ports of computers containing sensitive or classified information.

Desktop/Workstations are among the most common type of systems. They may run Windows, Linux, or other Intel hardware compatible Operating Systems and are generally known as PCs, or IBM compatible PCs. Apple Computers are similar, but are designed typically to run MacOS and applications. If they run a UNIX Operating System, they are generally referred to as UNIX boxes, and often have a different type of CPU than the PC. Hardware designed to use UNIX Operating Systems will not normally be able to run Windows Operating Systems. All these systems may run in a standalone mode or may be networked.

BASIC COMPUTING COMPONENTS

A computer system consists of four basic functions: input, output, storage, and retrieval.

Input: To *input* is to enter data into the computer generally through a peripheral device such as a keyboard, scanner, mouse or digitizer tablet.

Output: When we put something into the computer, we definitely want to get something back out. This could involve viewing a screen, identifying that information was processed, or transferring or transmitting from the computer to a peripheral device such as a printer, disk storage or to a communications line.

Storage: Storage is defined as the semi-permanent or permanent holding place for digital data. Permanent storage refers to disks and tapes and semi-permanent storage typically refers to Random Access Memory (RAM) chips. RAM is normally used as a temporary workspace for executing instructions and processing data.

Retrieval: To retrieve data is to call up data that has been stored in a computer system. When a user queries a database, the data is retrieved into the computer first and then transmitted to the screen.

Some people describe a fifth **processing** component. All information that is input, output, stored, or retrieved at one time goes through the Central Processing Unit.

THE CENTRAL PROCESSING UNIT

Now let's talk about the heart of a PC, the **Central Processing Unit (CPU)** which is also known as a microprocessor. To get into the typical desktop computer, we have only to undo a few screws in the back of the box and slide the cover off. When we do that, we see several items. The first item we see will probably be the **motherboard**. The motherboard, also called the "system board," is the main printed circuit board in an electronic device, which contains sockets that accept additional boards. In a desktop computer,

the motherboard contains the CPU, chipset, PCI (Peripheral Component Interconnect-input/output device) bus slots, AGP (Accelerated Graphics Port) slot, memory sockets and controller circuits for the keyboard, mouse, disks and printer. It may also have built-in controllers for modem, sound, display and network, obviating the need to plug in a card. A laptop motherboard typically has all peripheral controllers built in. Printed circuit boards that plug into another printed circuit board, such as the motherboard, to augment its capabilities are referred as **daughterboards**. Depending on the design, these boards control hard drives, floppy drives, scanners, modems, and any number of devices comprising the computer system.

As mentioned, there are many chips on the motherboard, but probably the most important is the microprocessor (i.e., CPU) chip (e.g., Pentium, Athlon, 486, etc.). This chip is so important that many times the computer is referred to as a “Pentium” computer, a “486” computer, etc. This is the component of the computer that directs all of the other computer operations. It reads the programs (software) and directs the rest of the computer to actually perform whatever the software directs (e.g., word processor, spreadsheet, database, etc).

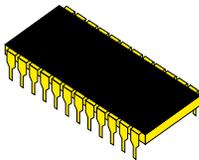
The last component of the CPU is **main memory**. Main memory is also known as main or primary storage. To understand how main memory functions, let's compare it to a desktop. Let's say that you have just so much space on your desk - just as you have only so much memory in your computer. If you take reference materials from a bookshelf and place them on your desk, you can only fit so many books on your desktop. Once you have covered your desktop, you cannot fit any other materials on your desk unless you close a reference book and return it to the bookshelf. The same thing happens within the computer system. Once its memory is full, it has to put something away before it can load something new. Normally the information will be moved to the hard drive for either temporary or permanent storage. Main Memory is not generally considered to be a permanent repository of information (although sometimes it may be and we'll talk about that in the next section, “States of Memory”). The security implication of the CPU is that everything goes through it - any and all information that is processed on a computer system, at some point in time, is stored in, or cycled through, main memory.

STATES OF MEMORY

Memory is of two types: volatile and non-volatile (sometimes called semi-permanent and permanent). **Volatile** means that the system's memory loses information when power is removed from the system by flipping a switch, pulling a plug, etc. **Non-volatile** means that the system's memory retains information when power is removed from it. This can be accomplished in various ways. One way may involve the use of a battery that backs up the memory chips. Several memory expansion boards may contain batteries that supply continuous power to the memory. Be very cautious of this, as there is a real security vulnerability associated with this type of memory. Since the information, which has been placed into non-volatile memory, will not be purged when power is removed, the next person who initiates a processing session on this type of system may find all of the previous person's material still contained within the system. After processing sensitive information on a system with non-volatile memory, we must be sure to remove all of the sensitive information from the system before leaving it in an uncontrolled or unprotected area. In the case of a battery backed-up system, the battery would have to be removed or a device (toggle switch) may be placed between the battery and the memory it protects. Other types of non-volatile memory, like flash memory, require no power. Once the information is written to these types of memory, it stays there until it is physically overwritten or removed.

SIZE OF MEMORY

The size of the memory is typically not a major security concern. However, there are times when the amount of memory available to the system and the amount of memory required by the software can create certain capabilities and vulnerabilities. If you need to run two programs each requiring 80MB of memory on a machine that only has 128MB of memory, it is easy to figure out that there is not enough memory on the system to accomplish this task - unless the system is a **virtual memory system**. Virtual literally means, "as needed." This type of computer system swaps out information that is contained in main memory to the hard disk where it is temporarily stored until it is needed again. Think of virtual memory as pseudo-memory. The swapping of information between main memory and hard disk storage is



done “transparently” to the user. This capability may create a security vulnerability because the system normally will not go back and overwrite the swapped out information when it is no longer needed. The computer may just label the spaces as unallocated, available for use by any system resource or object. An individual with access to the system and the proper utility tool could very easily recover and gain access to the information. It is very important that control be exercised over where the computer writes this information. Some utility programs on the commercial market will allow you to overwrite all unused storage locations. That will, in effect, clear the information that had been written to the storage media. In addition some Operating Systems are designed to either protect this information from access or overwrite it both in memory and on disk.

PERIPHERAL DEVICES

Hardware components other than the CPU are **peripheral devices**. These could include **disk drives, printers, monitors, keyboards**, and the like. Peripheral devices are typically considered to be on-line or off-line. They are **on-line** when under the direct control of the system (the CPU) and **off-line** when they are not under this control. This is an important concept to understand because there are serious security concerns associated with peripheral devices. You need to identify what components are being written to and where information is being stored. You also need to identify whether or not the CPU has the ability to task and utilize a certain peripheral device. If you don't want a peripheral device to be used when processing sensitive information, you have to disconnect it. The procedures for disconnecting these devices are discussed in the "Disconnect Methods" section.

TYPES OF MEMORY

In a previous section we identified the two states of memory. Now we'll discuss the two types of memory. These are read only memory and random access memory.

Read Only Memory (ROM) is permanent and, once information is written to a memory device, it stays there until that device is usually physically destroyed. The ROM content is created in the last masking stage of the chip manufacturing process, and it cannot be changed. Stand-alone ROM chips

and ROM banks in microcontroller chips (a single chip that contains the processor, RAM, ROM, clock and I/O control unit—a computer on a chip) are used to hold control routines for a myriad of applications. ROMs are also widely used to hold initial start-up software in PCs as well as plug-in cartridges for video games. When you turn a computer system on, ROM comes up and does the diagnostics, checks to make sure that the memory and disk drives are functioning properly, and then turns control over to the OS. You may read from the chip but you can never write to it. Since the user cannot write to ROM, any devices containing sensitive data have to be physically destroyed. This may be done by chemical decomposition, melting, grinding, or in some cases "popping" the ROM. Popping is accomplished by placing a ROM into a ROM or PROM (Programmable Read Only Memory) programmer and sending a destructive current (or surge) through the device. You must be authorized to use this method before destroying sensitive information.

There are various types of ROM. There's PROM (Programmable Read Only Memory) which can be programmed once by a user. The program then stays on the chip until it is destroyed. PROM is destroyed in the same fashion as ROM. Another device is EPROM (Erasable Programmable Read Only Memory). We have the ability to erase this device and use it again. It is normally erased with an ultra-violet light. It can be destroyed in the same fashion as ROM and PROM. Another type of ROM is EEPROM (Electrically Erasable Programmable Read Only Memory). EEPROM may be declassified by overwriting all storage locations containing sensitive information. PROM, EPROM and EEPROM are often used in weapons systems. So, if you're working with weapons systems, there is a very good chance that you will be involved with these devices and responsible for their protection.

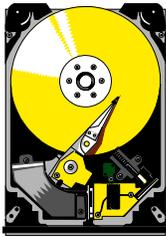
Random Access Memory (RAM) is the type of memory with which you are most familiar. It's the memory that you interact with when you're using your system. It is the real workhorse of the computer as far as memory goes. Information placed on a RAM chip can be moved around, transferred in and out, and erased.

You should be aware of what a **RAM Disk** is and how it affects system security. A RAM Disk is not a disk at all. A previous section discussed how virtual systems use disk space to create pseudo-memory, resulting in

disks acting like main memory. With the creation of a RAM Disk, memory acts like disks. This occurs when the computer system is configured to set aside a chunk of memory and have it function as a hard disk storage device. There is very little security risk associated with RAM disks as long as the computer system's memory is volatile. If the computer's memory is volatile, all the information in it is lost when the power is removed. RAM disks become security concerns only when the computer system's memory is non-volatile.

STORAGE DEVICES

Storage devices can be temporary or permanent. When we think of a **temporary storage device**, we usually think of main memory. When we turn the system's power off, the information disappears. **Permanent storage devices** are such things as floppy disks, zip disks, magnetic tape, optical disks, CD's, hard disks, DVDs, digital audiotape, and



various other storage media on which we retain information for an extended period of time. Magnetic tape systems come in reels and cartridges of many sizes and shapes. Although still used in legacy systems, open reels have been mostly superseded by cartridges with

enhanced storage capacities. Magnetic tape systems are most commonly used as backup systems especially for more economical data archiving. But tapes have a disadvantage in that they are sequential storage devices.

That is, you have to bypass all the other files stored on the tape before getting to the information you desire. Disks, as compared to magnetic tape, have a real advantage in that they are random access devices. That is, you can go directly to the location where your information is stored. This speeds up recovery and/or access actions and is why disk drives are the most common form of on-line storage. Compact Disks-Read Only Memory or CD-ROM disks have been on the market for a number of years and have a capacity of about 650 MB. The ROM in CD-ROM acts like the ROM we discussed earlier. It is normally programmed in by the vendor or manufacturer and accessed as a read-only device from that time on. CD-ROM disks need to be destroyed when they become unusable or damaged,

as there is no other approved way to purge the information from the media. CD-R and CD-RW disks can be written to by having the proper CD drive and software in the computer. The CD-R can be written to only once while the CD-RW can be written to numerous times and used much like a floppy disk. DVDs have a much larger capacity of 4 to 17 GB. They can be used like a CD with the proper drive and software.

Some of the newer storage devices use external flash memory such as in portable Universal Serial Bus (USB) storage devices. Many of these devices are very small; the size of key chains and credit cards and can hold several GB of memory.

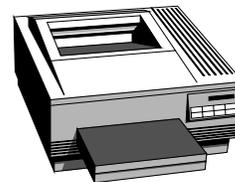
INPUT DEVICES

Before we can place information into the computer, we need some sort of input device. The most commonly used input device is the **keyboard**, but there are others. The computer **mouse** is very popular because it's used in conjunction with various graphical user interface (GUI) systems. The mouse has a track ball that runs a cursor on the screen across an X-Y axis. There's also a **light pen**. You touch the light pen to the monitor; it senses the location (X-Y axis) of the pen and executes a command based on this location. There are **touch sensitive screens** where you touch the monitor and it activates or executes a command based on the position of your finger. This is not an all-inclusive list of input devices, but examples of different types.



OUTPUT DEVICES

Printers, plotters, magnetic storage devices, modems, and Network Interface Cards (**NICs**) make up the vast majority of output devices in use today. **Printers** and **plotters** provide us with hard copy (paper) printouts. Whenever we create or modify a file, we normally save it to some sort of storage medium, e.g., a **floppy disk**, **zip disk**, **fixed disk** or **tape backup cartridge**. **Facsimile boards** that fit inside of today's microcomputers allow us to "fax" messages.



A **modem** or network interface is an extremely popular form of output device that enables us to share information with computers in other cities, states and countries. The NIC allows us to network our systems locally or if connected to a Cable Modem or DSL Modem over wide area networks. These are but a few of the output devices currently available. The security implications of output devices are clear. If sensitive information is being sent to these device(s), they need to be in secure areas or under the control of authorized individuals, and the lines over which they communicate must be protected or the signals appropriately encrypted.

INPUT/OUTPUT (I/O) DEVICES

Some devices such as **disk drives**, **NIC's** and **modems** constitute what are commonly referred to as input/output (I/O) devices. They do both input and output functions. These devices are subject to significant security vulnerability since most information is, at one time or another, stored on or read from these devices.

TELECOMMUNICATIONS

External communications security is a continuing problem in the DOD. We must communicate, but we need to be aware of how and where our information is being transmitted. Several methods allow computers to communicate. **Fiber-optic cable** is one transmission medium that is commonly used.



Information is sent as light pulses that travel through strands of glass tubing. Another transmission method is utilizing **microwave links**. Some U. S. telecommunications traffic goes through microwave links every day, either via the physical wires on telephone poles or via the satellite dishes that bounce these data and voice transmissions off of satellites. Whenever sensitive information is transmitted outside of a facility, it must be encrypted through a National Security Agency (NSA)-approved encryption algorithm. A Communications Security (COMSEC) account or a Seed Key Only COMSEC Account (SOCA) is required to obtain an approved encryption algorithm.

Wireless networking within a facility, using Infrared (**IR**) or Radio Frequency (**RF**) is becoming a very prevalent form of communicating among different devices and systems. The specific technologies may have different names but fall into the two general categories. Both forms present a security risk because they can be easily intercepted by someone other than the intended receiver.

Many laptops, palmtops, and PDA type devices have **IR** and/or **RF** capability. A person carrying them into an area where sensitive information is being transmitted via one of these methods could intercept information, or gain access to a wireless network. Unauthorized access to sensitive data or the perpetrating of malicious acts might be the result. With RF networking a person could be out in the parking lot and access the network or copy the information. You need to know what type of devices are coming into areas where sensitive information is being processed, either on a temporary or permanent basis.

Wireless communications should be encrypted and access to wireless networks should be controlled. If classified information is transmitted via wireless methods, the encryption must be NSA Type 1.

DISCONNECT METHODS

There are two ways to disconnect remote devices before processing sensitive information. The first is through software and the second is through physical.

Software disconnects provide a "logical" means of disabling certain resources of the computer system so that they cannot be used when sensitive information is being processed. For example, if you had 15 disk drives attached to a large-scale system and you wanted to use only one when sensitive information is being processed, the others would need to be disconnected. There is more than one way of accomplishing this. The computer can be programmed to recognize only one drive (and that is the drive to which it writes), or it can recognize all 15 drives, but be instructed to write to only one. Software disconnects must be verified and are not authorized for Top Secret accredited systems. Trust should not be granted as easily to a software disconnect as to a physical disconnect.

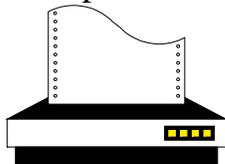
Physical disconnects can be accomplished by physically unplugging the device at the computer facility or by using a data switch. A data switch is a toggle type device with numerous positions and contacts so that a single communication port on a computer may communicate with various devices without having to physically unplug or reattach a cable. To communicate with a given device, all you have to do is turn the switch from one position such as "A" to another position such as "B." This action completes the circuit and allows the computer to be able to communicate with the given device. Some prefer this method over constant plugging and unplugging of cables to prevent connectors from being damaged.

TEMPORARY FILES

Temporary files are used for a variety of reasons such as to facilitate printing of large text files or graphics. They are normally written to storage media and can cause security concerns. Once a graphic has been printed, that temporary file may or may *not* be removed from the computer system's storage devices. Even when removed, the information in the temporary file remains since the removal is normally conducted by "deleting" the files which does not actually remove the file from disk. Deleting the file normally only identifies that space as unallocated and allows the system to utilize it when needed in the future. Word processors are infamous for writing temporary files. If you do a spell check of a document, you are asked (if necessary) to make corrections. If you make corrections, the system may ask you, "Do you want to save the information that's being changed or modified?" In most cases, this information (once you make the corrections) will be written to a temporary file somewhere on your hard disk. Most modern operating systems such as Windows, Linux or UNIX use temporary files for virtual memory. In addition, most web browsers (e.g., Internet Explorer) generate substantial numbers of temporary files.

PRINTER TECHNOLOGIES

There are two types of printers, impact and non-impact printers. **Impact printers** are printers such as dot matrix printers. The **dot matrix printer** has a print head that has either 9 or 24 pins. These pins look like needles and they hit a ribbon leaving impressions on the paper, which form characters. If you're processing sensitive



information using impact printing devices, be aware that a latent image remains on the ribbon. These ribbons must be appropriately protected. These types of printing devices are becoming more and more uncommon.

Non-impact printers include devices such as ink jet printers, plotters, thermal printers and laser printers. **Ink jet printers** form characters by squirting ink through a nozzle onto paper. A **plotter** grabs a pen and runs it across paper or acetate, creating either text or graphical images. These devices do not use ribbons or leave behind latent images.

Another type of non-impact printer uses a thermal transfer type of technology. Normally, when we think of a **thermal printer**, we envision a traditional fax machine which has a thermal transfer device that imparts, on specially coated paper, images that we can read in the form of characters and/or graphics. Thermal transfer devices such as color laser printers have either three or four-color ribbons. The three-color ribbons are red, green and blue (RGB); the four-color ribbons are cyan, magenta, yellow and black (CMYK). These printers run a heated ribbon or film across a page to place images on the page and then transfer a mix of colors to form the appropriate colors for the images. Since a negative type of image remains on the ribbon, it must be protected after processing sensitive information. So either the ribbon has to be removed from the printer or the printer will have to be safeguarded in an approved storage location. This type device is rather rare.

Laser printers are very popular because of their high resolution. This printer works by using a laser to charge a magnetic drum. The drum then rolls across the paper, magnetically charging the paper, which attracts the toner, and then a fixing agent fixes that image in place on the paper so that it doesn't smear when it comes out of the printer.



In order to properly sanitize laser printers, removing power is generally all that is required; however, if the print cycle is not completed (e.g. paper jam or power failure) one page of print (font test acceptable) must be run. Output can be disposed of as unclassified if visual examination does not reveal any classified information. Do not send blank pages through the laser printer because most laser printers, when receiving a signal from the computer to

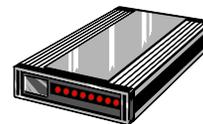
print a blank page, may execute a form feed which has no affect upon any latent image on the printing drum.

Laser printers usually have very large buffer devices. **Buffers** are memory devices which compensate for the exchange rate between the very fast computer and very slow mechanical devices such as printers or modems. To ascertain the characteristics of your laser printer's buffer, you should contact your vendor or the laser printer's manufacturer. Given that information, you will know how long to protect the equipment after processing sensitive information to ensure that any data in the buffer is removed before reuse. It is also possible for a high-end printer or copier to have a disk drive (non-volatile storage). This will further compound the security problems.

The security implications of printer technologies include possible latent images on the ribbons, on thermal wax paper, and drums. After processing sensitive information, we need to protect any information that remains or take precautions to ensure that none is left behind.

MODULATOR/DEMULATOR (MODEM)

MODEM stands for **M**odulator and **D**emodulator. A MODEM is a device that allows a computer or terminal to transmit data over a standard telephone line. Computers work with digital signals. Digital information is sent from the computer to its local modem. The local modem changes the digital signal to an analog signal. This is known as modulation. The signal is then sent via communications links to the remote modem. Upon receipt, the remote modem changes the signal from an analog signal back into a digital signal. This is known as demodulation. If you want to find out whether or not a system has a modem, look at the backside of the computer for a little modular phone jack like the one you have in your home. If you see a modular phone jack, there's a very good chance that the system has a modem, but make sure that you're not looking at the system's connection for a local area network since these connections are similar. The best way to determine whether the system has a modem is to let the system itself tell you. In a Windows system go to the Control Panel. If there is an icon for Modem, click on it and see what it tells you. In addition you may also go to the System icon and look for a modem under the Device Manager tab. Since



UNIX Operating systems are unique, ask the System Administrator how to determine if the system has a modem.

FAULT-TOLERANT SYSTEM (S)

Computer work stoppages are usually critical because we cannot afford any downtime in the computer system - whether in the commercial or military environments. Let's say that you called an airline to make a reservation and were told, "I'm sorry but our computer's down, call us back in an hour." Chances are you would call another airline to book a flight. Or, if you were commanding forces in a regional conflict and required instant information, an inoperative system might be life threatening. When we can't afford for systems to go down, we create **fault-tolerant systems**. They may also be called high availability, backup, redundant, or mirror systems. Fault-tolerant systems are two or more identical components that are placed in a system so that if one fails, the other one automatically takes over and allows the system to continue processing. If these systems are used to process sensitive information, the same security concerns and requirements apply to both systems. If one goes down and the other takes over, the information that was on the first device is now on the second device, so we have to control them both. If the media has to be marked on one device, it has to be marked on the other device. If information has to be brought into accountability on one device, it has to be brought into accountability on the other device. So don't overlook the duality of requirements for these systems.

MODIFICATIONS MAY LEAD TO PROBLEMS

Computer technology is constantly evolving and systems are changed to take advantage of improved capabilities. The continuous control of changes made to a system's hardware, software, firmware and documentation throughout its life is called **configuration management**. You need to be aware of how the computer system is modified because certain changes affect security, particularly if the system is approved (accredited) to process sensitive information.

Memory is always being expanded. Usually the more sophisticated a software program is, the more memory it requires to run. Adding memory to the system (as discussed earlier), doesn't necessarily cause a security problem. But, if we were to change the memory of a system from volatile to non-volatile, the security of the system would be affected. The security controls exercised over that system to address the process for clearing memory would no longer be adequate. All non-volatile memory devices



must be sanitized of sensitive information prior to releasing them from the controlled area.

When a system is modified, its security procedures - those in practice and those in writing (the approval/accreditation documentation)- must be re-evaluated.

Another area that may create security concerns involves resource sharing. Peripheral devices tend to be very expensive and may have many computers hooked up to them. If another computer is connected to a printer that is part of an approved (accredited) system, the security of the system is affected. The system security procedures must now identify how users of this computer will be excluded from access to the system when sensitive information is being processed.

Changes in peripherals may or may not affect the security of the system and may or may not require reapproval (re-accreditation) of the system to process sensitive information. The replacement of an impact printer with another impact printer may have little affect, if any, on the security of the system since the security procedures associated with these two devices are quite similar. (Ribbons need to be removed and secured. The buffer device in both are normally volatile so power must be removed from the printer to clear its memory.) However, the change from an ink jet printer to a thermal transfer printer would normally require a rewrite of security procedures and reapproval (re-accreditation) as a result of the difference in their technologies. (Because the ink jet printer uses no ribbon, procedures for protecting the ribbon would not be necessary.) Going from an inkjet printer to a laser printer with a drum (which must be removed or overwritten) would normally require a rewrite of security procedures and reapproval (re-accreditation).

Modifications of storage devices can also cause security problems. If a system's removable storage media such as floppy disks, cartridge disks, or Zip disks were replaced with a fixed, non-removable hard disk, the security concerns would change significantly. This type of change normally requires reapproval (re-accreditation) of the system.

Backups can cause concern. Sensitive information *should* be backed-up frequently. As long as the same security requirements that apply to the originals are applied to the backups, there should be no security problems. (If the original is classified, protected at a certain level and entered into accountability, the backup will also be classified, protected at the same level and entered into accountability.) The backup, however, should be secured in a location other than the one where the primary (original) storage medium is retained. That way, if a localized natural disaster such as a fire or flood occurs, this resource will not be damaged along with the original. The only time backups of sensitive information should *not* be made is when the program manager specifically prohibits it.

SECURITY IN REVIEW

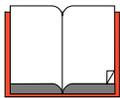
Let's review some of the security concerns associated with information systems:

- It is important for us to know from what source (media, workstation, etc.) the computer is reading and to what destination it is writing. It does us very little good to secure the local computer hardware and software when the system is sending (writing) information to a remote device (printer, plotter, terminal) which is not protected.
- It is important to know what type of communications are available to the system; e.g., wire, fiber-optic, Infrared, or Radio Frequency.
- We are concerned with latent images on output devices such as laser printer drums and color thermal film/ribbon.
- It is important to know the kind of memory the system/peripherals have and how must it be sanitized.

- If the system has the ability to temporarily write information to storage media (virtual memory systems/temporary files, etc.), then we need to control where the information is written and be able to modify and/or override these system characteristics.
- Any changes to a removable storage device causing it to become a fixed storage device should be addressed immediately.

RESOURCES AVAILABLE TO YOU

When it's necessary to find out what characteristics or capabilities a system



has in order to determine appropriate security procedures, try referencing the system's operating manuals. For complicated systems, such as minicomputers and mainframes, this documentation may be voluminous. However, in most cases, the information that you need will be found in one of these documents. Sometimes, you can rely on a technical representative of your organization to steer you to the right information. If for some reason you can't lay your hands on the documentation, talk with the employees who are most familiar with the system. In most cases, these employees know how the system works and can give you the required information. When you run into a situation where the employees don't know, ask the vendor. The vendor should be able to help you. Also, don't forget about the computer specialist in your organization/agency. If you have one, this person sees a multitude of systems and can be a wealth of information and knowledge when it comes to answering your questions.

There are many sources of information that may help answer any questions you might have: 1. Computer user-related magazines. 2. Computer classes (basic introduction to computers and office automation - not necessarily programming courses) at local universities. 3. The technical people in your organization/agency. (Our experience has been that these people are usually very good at sharing their knowledge, but they cannot help until asked.) 4. Local computer users groups. 5. Web Sites.

CONCLUSION

This booklet is not designed to be an "everything you wanted to know about computers, but were afraid to ask." Its purpose is to introduce you to computer terminology and technology, and to get you thinking about security issues associated with information systems. We hope that some of your questions about computers and security have been answered.

Any comments or suggestions on ways to improve this booklet should be directed to dssacademy@mail.dss.mil.



INDEX

A

ASK FOR ASSISTANCE..... 3

B

BASIC COMPUTING COMPONENTS 12
BIOS..... 5,6
Bit..... 5
BITS AND BYTES..... 5
BOOTING THE COMPUTER 5
Buffers..... 23,25
byte..... 5

C

CATEGORIES OF MICROCOMPUTERS 10
CD-ROM *See* Compact Disks-Read Only Memory 17,18
CENTRAL PROCESSING UNIT 12
CF..... 4,21
cold boot..... 5,6
Compact Disks-Read Only Memory..... 17,18
compiling 7
CONCLUSION 28
configuration management..... 24
CPU *See* Central Processing Unit..... 6,9,11,12,13,15

D

daughterboards 13
DISCONNECT METHODS 20
dot matrix printer 21

E

EEPROM	16
Electronically Erasable Programmable Read Only Memory.....	16
EPROM.....	16
Erasable Programmable Read Only Memory	16

F

FAULT-TOLERANT SYSTEM	24
Fiber-optic cable	19,26
Firmware	4,5,24

G

general purpose computers	8
---------------------------------	---

H

hardware.....	3,4,5,7,11,15,24,26
HARDWARE/SOFTWARE/FIRMWARE	4
High level languages.....	7

I

I/O	16,19
Impact printers	21,22
Ink jet printers	22
Input	5,12,18,19
INPUT DEVICES	18
INPUT/OUTPUT DEVICES	19
INTRODUCTION	3

K

keyboard.....	6,10,11,12,13,15,18
---------------	---------------------

L

LANGUAGES	6
laptop computers.....	9,10,13,20

Laser printers.....	22,23,25,26
light pen.....	18
low level language	7
luggable computer.....	10

M

machine language.....	7
main memory	13,14,17
mainframe computer	9,10
microcomputer	9,10,19
Microwave links.....	19
minicomputer	9,27
MODEM <i>See</i> Modulator/Demodulator	4,7,13,18,19,23,24
MODIFICATIONS MAY LEAD TO PROBLEMS	24
MODULATOR/DEMODULATOR	23
motherboard	6,12,13
mouse	12,13,18

N

Non-impact printer.....	21,22
Non-volatile	14,17,23,25
notebook computers	10

O

OS <i>See</i> Operating System	4,5,7,8,11,15,21,24
off-line.....	15
on-line	15,17
OPERATING SYSTEM	4,5,7,8,11,15,21,24
Output.....	5,12,18,19,22,26
OUTPUT DEVICES	18

P

Palmtop computers.....	10
PC	5,6,7,8,9,10,11,12,16
PDA.....	10,20
PERIPHERAL DEVICES.....	15

Permanent storage	4,12,13,15,17
Personal Digital Assistants <i>See</i> PDA.....	10,20
Physical disconnects	20,21
plotters.....	9,18,22,26
Portable computers.....	10
PRINTER TECHNOLOGIES.....	21
Printers	7,9,12,13,15,18,21,22,23,25,26
processing.....	4,8,9,12, 14,15,20,21,22,23,24
Programmable Read Only Memory	16
PROM <i>See</i> Programmable Read Only Memory	16
Pseudo-memory	14,16

R

RAM.....	5,6,12,16,17
RAM Disk	16,17
Random access memory.....	5,12,15,16
Read only memory	4,15,16,17
remote.....	4,20,23,26
RESOURCES AVAILABLE TO YOU.....	27
Retrieval	12
ROM <i>See</i> Read only memory	4,15,16,17

S

SECURITY IN REVIEW	26
SIZE OF MEMORY	14
SIZES OF COMPUTERS:.....	9
software	3,4,7,13,14,16,18,20,24,25,26
Software disconnects	20
Special purpose	8
STATES OF MEMORY	14
Storage	3,4,5,9,10,12,13,14,16,17,18,21,22,23,26,27
STORAGE DEVICES	17

T

Tablet PC.....	10
TELECOMMUNICATIONS.....	19
TEMPORARY FILES	21

temporary storage device	17
thermal printer	22
touch sensitive screens	18
TYPES OF COMPUTERS	8
TYPES OF MEMORY	15

V

virtual memory system.....	14,21,27
volatile.....	6,14,17,23,25

W

warm boot	5,6
-----------------	-----



DEFENSE SECURITY SERVICE ACADEMY
938 Elkridge Landing Road
Linthicum, Maryland 21090
(410) 865-2295

Security through Knowledge