# Data and Information Security in a Global Age

Akintunde Michael Yinka

*Department of Electrical/Electronics Engineering*
*Tower Polytechnic, Ibadan, Oyo State, Nigeria*

*Abstract Having observed carefully the dynamics of e- activity and technology in business, finance and other realms of human endeavour, the issue of data and information security with computer networks becomes more relevant in order to keep up with the growing trend, hence the need to carefully address some important issues concerning data and information security. Information and data security, computer security are often incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting confidentiality, integrity and availability of information .Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Governments and other realms of human endeavour amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronics computers and transmitted across networks to other computer. Protecting confidential information is a business requirement and in various cases also an ethical and legal requirement. This article presents a general overview of information and data security and its core concepts in this era where e- activity and technology has been the prevailing trends in getting things done throughout the world.*

*Key words: data, information, due care, due diligence, information, information security, vulnerability, threat, access control, cryptography*

## Introduction

Since the early days of writing, everyone, heads of state and military commanders inclusive understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering.

Julius Caesar is credit with the invention of the Caesar ca. 50 B.C which was created in order to prevented his secret messages from being read should a message fall into the wrong hands. World War II brought about much advancement in information and data security and marked the beginning of the professional field of data and information security. The rapid growth and widespread use of electronic data processing and electronic business conducted through the internet, along with numerous occurrences of international terrorism, frieled the need for better methods of protecting the computers, data and the information they store process and transmit. The academic disciplines of computer security, information security and assurance emerge along with numerous professional organizations- all sharing the common goals of ensuring the security and reliability of information systems.

The end of the 20$^{th}$ century and early years of the 21$^{st}$ century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user.

As a result, the field of data and information security has grown and evolved significantly in recent years. It offers many areas for specialization including: security network and allied infrastructure, securing applications and database to mention but few.

## Definition of Terms

Data and information are often used as if they mean the same thing. Technically, they are different. Therefore, each and everyone of them will be well examined.

## Data

Data can be defined as the facts, events, activities and transactions which have been recorded. It is the raw materials from which information is produced.

## Types of Data

There are three main types of data which computer can store and process, they are:
(i). Numeric data (ii). Alphabetic data (iii). Alpha numeric data

Numeric Data: these are facts, events, activities and transactions that has been recorded in form of numbers or figures which can be subjected to a range of arithmetic operations (such as addition, subtraction etc.) in their natural state without loss of meaning. Numeric data are also referred to as quantitative data. Examples of numeric data are inventory figures.

Alphabetic Data: these are the facts, events, activities and transactions that have been recorded in form of alphabet. It could be the name of a customer, customer addresses, and product names. It could also be a sentence, idioms etc. any data supplied to computer that are entirely made up of letters will be automatically recognized to be alphabetical data unless it is otherwise stated by the programmer. They cannot be subjected to arithmetic operations in their natural form.

Alphanumeric Data: these are the facts, events, activities, and transactions which have been recorded in form both alphabetic and number. They are made up of letters and digits examples are: vehicles plate number (AX105 BDJ) serials no of equipments and street numbers etc.

Information: data and information are often used as if they are the same. Technically, information can be defined as the data which have been processed to a meaningful end.

Information Security: this means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Vulnerability: this is the weakness that could be used to endanger or cause harm to an informational asset.

A Threat: this is anything (man made or act of nature) that has the potential to cause harm.
Due Care: these are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.
Due diligence: these are the continual activities that make sure the protection mechanisms are continually maintained and operational.

The definitions of both the due care and diligence was as offered in the field of information security by Harris

## Overview

The CIA triad i.e. confidentiality, integrity and availability have been known as the core principles of information security for over twenty years. Meanwhile, accountability has been proposed to be an addition to this classic trio.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad which he named the six atomic elements of information. The elements proposed are: confidentiality, possession, integrity, authenticity, availability and utility.

## Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or system. For examples, a credit card transaction in the internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear i.e. (database, log files, backups, printed receipts etc), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Firstly, permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorize to have the information

## Integrity

In information and data security, integrity means that data cannot be modified undetectably. Integrity is violated when a data is actively modified in transit. Information security systems typically provide information integrity in addition to data confidentiality.

## Availability

The information must be available when it is needed, in order for any information to serve its purpose. This implies that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DOS) attacks.

## Authenticity

In computing, e-Business, data and information security, it is necessary to ensure that the transactions, communication or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are; Electronic commerce uses technology such as digital signature and encryption to establish authenticity.

## Methodologies of Data and Information Security

There are two major methods of data and information security which will be discussed elaborately here; they are *Access Control* and *Cryptography.*

1. Access Control: - Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to

protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement *"Hello, my name is Chika Abdullahi"* they are making a claim of who they are. However, their claim may or may not be true. Before Chika Abdullahi can be granted access to protected information it will be necessary to verify that the person claiming to be Chika Abdullahi really is Chika Abdullahi

Authentication is the act of verify a claim of identity. When Chika Abdullahi goes into a bank to make a withdrawal, he tells the bank teller he is *Chika Abdullahi* (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has Chika Abdullahi printed on it and compares the photograph on the license against the person claiming to be Chika Abdullahi. If the photo and name match the person, then the teller has authenticated that Chika Abdullahi is who he claimed to be. There are three different types of information that can be used for authentication: something you know, something you have, or something you are. Examples of *something you know* include such things as a PIN, a password, or your mother's maiden name. Example of *something you have* includes a driver's license or a magnetic swipe card. *Something you are* refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans. Strong authentication requires providing information from two of three different types of authentication information. For example, something you know plus something you have. This is called two factor authentications. On computer systems in use today, the Username is the most common form of identification and the password is the most common form of authentication. Usernames and passwords are slowly being replaced with some sophisticated authentication mechanisms.

Meanwhile, after a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is known as authorization.

Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems are equipped with different kinds of access control mechanisms – some may even offer a choice of different access control mechanisms. The control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resources the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied base upon the security classification assigned to the information resource. Examples of common access control mechanisms in use today include Role-based access control available in many advanced Database Management Systems, simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers.

2. Cryptography: - Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called enciphered. The most prospective systems of cryptographic data protection are the systems with an open key. In such systems

data are enciphered using one key and deciphered using another key. The first key is not confidential and may be published for using by all users of the system who encipher data. Data deciphering with the help of this known key is impossible. To decipher data the receiver uses another key, which is confidential. It is clear that deciphering key can not be determined based on the knowledge of the enciphering key. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage. For example, in multimedia data transfer, RSA algorithm is one of the most prospective ciphering algorithms employed as depicted in the Figure 1 below. This is because the crypt resistance of RSA algorithm is based on the assumption that it is exceptionally difficult to determine the secret key by the known key,

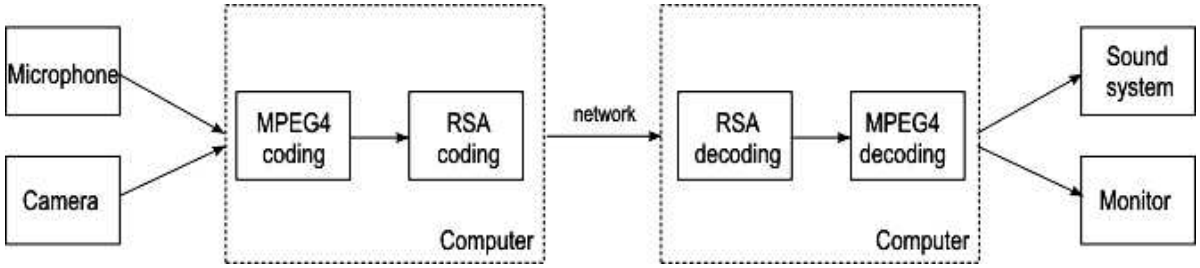


Fig.1 The procedure of data conversion

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure application such as telnet and ftp are slowly being replaced with more secure applications such as SSH that use encrypted network communications. Wireless communication can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key change. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.
Cryptography can introduce security problems when it is not correctly implemented. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography.

## Conclusion

Data and information security is the on going process of exercising due care and due diligence to protect information and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring and detection, incident response and repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.

## References

ALLEN, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X.

Krutz, Ronald L; Russell Dean Vines (2003). The CISSP Prep Guide (Gold Edition ed.). Indianapolis, IN: Wiley. ISBN 0-471-26802-X.

Layton, Timothy P. (2007). Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.

McNab, Chris (2004). Network Security Assessment. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.

Peltier, Thomas R. (2001). Information Security Risk Analysis. Boca Raton, FL: Auerbach publications. ISBN 0-8493-0880-1.

Peltier, Thomas R. (2002). Information Security Policies; procedures, and standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.

Dhillon, Gurpreet (2007). Principles Of Information Systems Security: text and cases. NY: John Wiley & Sons. ISBN 978-0471450566.