Analysis of Data Security Approach for Digital Computers

Aru Okereke Eze, Iroegbu Chibuisi, Enyenihi Henry Johnson

Department of Computer Engineering Michael Okpara University of Agriculture, Umudike, Umuahia, Abia State, Nigeria
Department of Electrical/Electronics Akwa Ibom State University, Akwa Ibom State, Nigeria

ABSTRACT: *This research is on the analysis of data security approach for digital computers.*
The three basic security factors to consider are Confidentiality, Integrity and Availability, while the concepts relating to the people who can access a particular data are authentication, authorization and non-repudiation.
The method of cryptography helps in securing information on the internet. Private and public key encryption ensure that only the intended recipient can read confidential information or have access to data.
This research analysis has aimed to act as a gadfly for future researchers to rely on.

KEYWORDS*: Data, Security, Confidentiality, Integrity, Availability, Authentication, Authorization, Cryptography, Encryption*

I. INTRODUCTION

Security incidents are on the rise everywhere. Hackers frequently break into corporate organization and even military systems. Internet was originally conceived of and designed as a research and education network, usage pattern have radically changed.

Most disturbing, modern internet hackers have automated hacking programs that allow even unsophisticated hackers to wreck havoc with corporate network and computers. Also, internal corporate break-ins by employees and ex-employees are still the biggest security problems in organizations. As internet has expanded into areas of commerce, medicine, commercial communication and public service, increase reliance on it is expected over the next few years, along with increased attention to its security. Since the information and tools needed to penetrate the security of corporate networks are widely available, network security has become a major concern for companies throughout the world.

Data security approach for digital computers are the techniques use in securing data (information) on a private digital computer network when connecting a private network to a larger network such as the internet.

This research “Analysis of data security approach for digital computers” x-rayed data security issues that arise when connecting a private network to the internet.

Section **II** of this research examines the literature review and theory of data security approach; Section **III** surveyed the methodology, design and implementation of security measures; Section **IV** presents the result analysis and discussion, while section **V** summarizes and concludes the work.

II. BACKGROUND REVIEW

The internet began in 1969 as the ARPANET, a project funded by Advanced Research Project Agency (ARPA) of the U.S Department of Defense. When internet was born, little thought was given to security. One of the original goals of the project was to create a network that would continue to function even if major sections of the network failed or were attacked and to reroute network traffic automatically around problems in connecting systems.

As more locations with computer joined the ARPANET, the usefulness of the network grew. By 1971, the internet linked about two dozen research and government sites, and researchers had begun to use it to exchange information not directly related to the ARPANET itself. The network was becoming an important tool for collaborative research, but it was rare that a connection from a remote system was considered an attack, because ARPANET users comprised a small group of people who generally knew and trusted each other.

In 1986, the first well-publicized international security incident was identified by Cliff Stoll, then of Lawrence Berkeley National Laboratory in northern California. A simple accounting error in the computer records of systems connected to the ARPANET led Stoll to uncover an international effort, using the network to connect to computers in the United States and copy information from them. In 1988, the ARPANET has its first network security incident, usually referred to as “the Morris worm”. In 1989, the ARPANET officially becomes the internet and moved from a government research project to an operational network. Security problems continued, with both aggressive and defensive technologies becoming more sophisticated.

Today, the use of the World Wide Web and Web-related programming languages creates new opportunities for network attacks. Intruders can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activities.

III. THEORY

The three basic security concepts relevant to data (information) on the internet are confidentiality, integrity and availability. The concepts relating to the people who use that data (information) are authentication, authorization, and non-repudiation. It is easy to gain unauthorized access to data in an insecure networked environment, and it is hard to catch the intruders. Examples of important information are passwords, access control files and keys, personnel information and encryption algorithms.

When information is read or copied by some unauthorized person, the result is known as loss of confidentiality. Also when information is modified in unexpected ways, the result is known as loss of integrity, while when information is erased or become inaccessible, the result is loss of availability. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted, the user cannot later deny that he or she performed the activity. This is known as non-repudiation.

IV. DESIGN METHODOLOGY AND IMPLEMENTATION OF SECURITY MEASURES

In the face of vulnerabilities and incident trends, a robust defense and protection measures becomes necessary and required flexible strategies that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.

4.1 Encryption

The most basic building block of security is encryption, which scrambles a message before transmission, so that an interceptor cannot read the message as it flows over the network. However, the receiver knows how to decrypt (descramble) the message, making it readable again. Encryption provides privacy, which is called confidentiality. Both terms means that message can be transmitted without fear of being read by adversaries.

Encryption methods falls into two categories (symmetric key encryption and public key encryption), with numerous specific encryption algorithms.

4.2 Symmetric key encryption

Symmetric key encryption has a single key that is used by both communication partners. Figure 1 shows a symmetric key encryption method.

- When party A sends to party B, party A encrypts with the single symmetric key and party b decrypts with the same key.
- When party B transmits to party A, in turn party B encrypts with the single symmetric key and also party A decrypts with the same key.

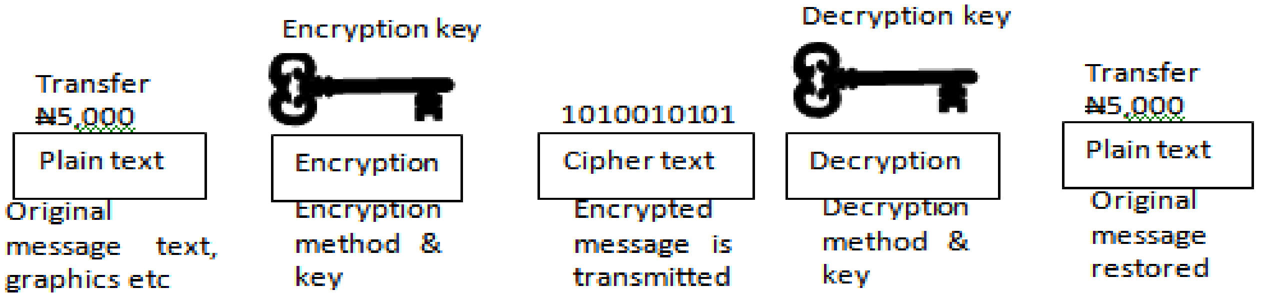

Figure 1: Symmetric key encryption

4.3 Public key encryption

In public key encryption, when one party sends to another, there are two keys; the receiver public key and the receiver private key. Both of the keys are those of the receiver, not of the sender.

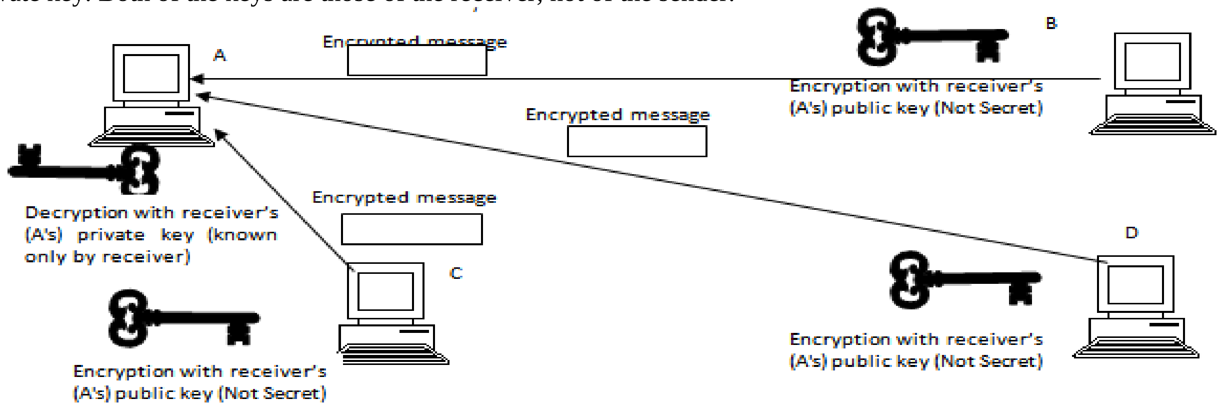
A
Encrypted message
B
Encryption with receiver's (A's) public key (Not Secret)
Encrypted message
Decryption with receiver's (A's) private key (known only by receiver)
Encrypted message
C
D
Encryption with receiver's (A's) public key (Not Secret)
Encryption with receiver's (A's) public key (Not Secret)

Figure 2: Shows a public key encryption method

4.4 Authentication

Authentication proves the sender's identity. If we get a message claiming to be from someone, we want to be certain that it is not really coming from someone else, we apply the concept of authentication. There are many forms of authentication; passwords authentication, authentication card, biometric authentication etc.

4.5 Hashing

Hashing takes a message of any length and computes a small bit string of fixed length. The two most popular hashing algorithms, MD5 and the Secure Hash Algorithm 1 (SHA-1), create hashes that are 128 bits and 160 bits long respectively, no matter how long the original message is. Hashing is different from encryption because, hashing is not reversible. It is a one-way function.

Other protective measures of safeguarding our network include; Integrated Security Systems (ISS), Multi Layer Security, Firewalling etc.

V. RESULT ANALYSIS AND DISCUSSION

From the design and implementation of security measures for digital computers emerge the following results.

5.1 Cryptography

One of the primary reasons why intruders are successful is that most of information they acquire from a system are in a form that can read and comprehend. Cryptography secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Also, cryptography checksums helps in preventing undetected modification by encrypting the checksum in a way that makes the checksum unique. To protect against the chance of intruders modifying or forging information in transit, digital signatures are formed, by encrypting a combination of a checksum of the information and the author’s unique private key.

5.2 Operational technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect security. No single technology addresses all the problems and threats. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

5.3 Security analysis tools

Because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A vulnerability identification tools are available, which have gained praises.

VI. CONCLUSION

This research work has analyzed data security approach for digital computers. It has attempted to present various attacks and vulnerabilities of data over the network, especially as the internet is a public network. Those affected by such attacks include banks, insurance companies, government agencies, network service providers, utility companies, universities etc. The consequences of a break- in cover a broad range of possibilities: decrease in productivities, loss of money or staff man hour, loss of market opportunity, legal liability etc.

In order to have a secured computer, both the network designer and IT security teams should work hand in hand to develop a security architecture that would be integrated into the existing enterprise network.

REFERENCES

[1] Annabel Z. Dodd. The essential guide to telecommunication, second edition.

[2] Caelli, W., Longley, D., and Shain, M., Information Security Handbook, Stockton Press, New York, 1991.

[3] CERT coordination center, CERT advisories and other security information, CERT/CC, Pittsburgh, P.A. Available on line: http://www.cert.org.

[4] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O’ Reilly & Associates, Sebastopol, C.A, 1995.

[5] Denning, P.J. ed., Computers Under Attack Intruders, Worms and Viruses, ACM Press, Addison-Wesley, New York, 1990.

[6] Garfinkel, S., and Spafford, G. Practical UNIX and Internet Security, 2nd ed, O’Reilly & Associates, Sebastopol, C.A. 1996.

[7] Kaufman, C., Perlman, R., and Speciner, M., Network Security: Private Communication in a public world, Prentice-Hall, Eaglewood Cliffs, NJ, 1995.

[8] National Research Council, computer at risk: Safe computing in the computer Age, National Academic Press, Washington D.C., 1991.

[9] Randall K. Nicholas/ CSA Guide to cryptosystems McGraw-Hill 199, page 248

Aru, Okereke Eze is a lecturer in the Department of Computer Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. His research Interests include Computational Intelligence, Computer Hardware design and maintenance, Security system design, , Expert systems and Artificial Intelligence, Design of Microcontroller and Microprocessor based system, digital systems design using microcontrollers and other computer related subjects.

Iroegbu Chibuisi is a postgraduate student in the Department of Computer Engineering, Michael Okpara University of Agriculture, Umuahia, Abia State, Nigeria. Her research interests include Computer Hardware design and maintenance, Security system design, etc.

Enyenihi Henry Johnson is a lecturer in the Department of Electrical/Electronics Engineering, Akwa Ibom State University, Akwa Ibom State, Nigeria. His research interests include Computer Hardware design and maintenance, Electronic and Communication Systems, Data Communication system designs etc.