

Application of Cryptography for Information Security in Umaru Musa Yar'adua University, Katsina-Nigeria

¹Abdulrashid Abubakar, ²Zakarai Mohammed, ³Babangida Dandgani Umar

¹Department of Library and Information Science Federal University, Dutsinma

^{2,3}Department of Library and Information Science, Ahmadu Bello University, Zaria

¹abubakarabdulrashid@rocketmail.com, ²zakmoh2000@yahoo.com, ³nadangani44@yahoo.com

Abstract

This study investigated the application of cryptography for information security in Umaru Musa Yar'adua University, Katsina. Two research objectives were formulated and answered. These were: To examine the extent to which cryptography has prevented the security breach of electronic databases and to identify the challenges encountered in the application of cryptography in UMYUK Katsina. The population of the study comprised all the staff members of the Directorate of Information and Communication Technology in the study area. Since the population is not too large, all 21 staff were used as the sample for this study. The questionnaire was the instrument used to collect data for this study. The data collected were presented and analyzed using frequency distribution tables and percentages. The study found that poorly designed user interface, quality of encryption, denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions, and speed of encryption were the common challenges encountered in the application of cryptography. This study recommended that the Directorate of ICT should, as a matter of policy, mount a regular training programme such as seminars, workshops, symposia, and in-house IT training for their staff to equip them with the latest development in the areas of information security systems to provide means of detection and remediation of security breaches of databases such as phishing scams and the like.

Keywords: Cryptography, Information Security, University, Security Breaches, Security Threats

Introduction

The introduction of computers, together with the development of Internet technology, has change how organizations handle and secure there. Mohammed (2012) conceptualized information as “whatever we physically or otherwise come across consciously or unconsciously, accidentally or intentionally and regularly or occasionally that adds positively or otherwise to our existing knowledge; education and training; curricula; skills; practices; ideas; ideals; culture; tradition; belief; expectations; experiences and wellbeing.” "One of the main paradigm shifts of the emerging information society is that information is becoming crucial if not the most important resource” (Maurer, 2004). information Abubakar (2014) remarked that “information is

currently created, stored, preserved and transmitted in electronic format. Electronic information is the lifeblood of many organizations and consequently needs to be suitably protected. This is especially important in an increasingly interconnected academic environment where information is now exposed to a growing number and a wider variety of threats and vulnerabilities”.

Menezes, Van Oorschot, & Vanstone (1997) affirmed that "security is necessary when communicating multimedia data over any untrusted medium such as public networks, and in particular, the Internet to protect information from theft, alteration or misuse."

“Information security is such a broad discipline that it's easy to get lost in a single area and lose perspective” (Miessler, 2013). “Information security is concerned with the confidentiality, integrity, and availability of data regardless of the form the data may take: electronic, print, or other forms” (Savu, 2013). Similarly, Schneider (2013) saw information security “as a means of protecting information and information systems from unauthorized access, use, disruption, or destruction."

Advancements in Information Technology (IT) have enhanced universal electronic connectivity, which poses new challenges to security, such as social engineering, phishing, viruses, hacking, electronic eavesdropping, and electronic fraud; there is no time at which information security does not matter. Cybercriminals are clever, innovative, well-financed, and technically proficient and are willing to take extraordinary efforts to attack information systems. To combat them, there is the need to be familiar with their tactics and techniques, learn how to safeguard the information, and follow the best practices concerning information security. Achieving information security in an academic environment requires a vast array of technical and legal skills. The technical means to deal with information insecurity, particularly information stored in a database, is provided through cryptography.

“Encryption is so important for data security. Even if an intruder could gain access to institutions’ network or even mobile device containing sensitive data, the data would be unreadable unless they also had access to the encryption key that unscrambles the data” (Schneier, 1997). “Data encryption solutions are built on a proven and scalable crypto foundation that makes it possible to efficiently protect the data assets themselves, allowing organizations' data to move freely and securely through any medium” (SafeNet, 2014). “While no one can guarantee 100% security, cryptography can help significantly. The good news is that if an organization already has the algorithms and protocols, it can secure its systems; the bad news is that implementing the protocols successfully requires considerable expertise” (Schneider, 2013). “There is currently a widespread engineering effort to incorporate cryptography into various aspects of the Internet. Most of the difficulty in engineering cryptographic systems has to do with understanding the trust relationships between different entities involved in a protocol” (Murphy and Badger, 1996)

Problem Statement

The success of any organization depends on how to secure the data stored in their databases is “In academic environments, databases contain personal profiles, academic

information about students, which are usually classified as sensitive. Often, the identity of an individual is stored in the database whether by name, personal code or a combination of attributes” (Bagdanov, 2007). “Databases and their applications form one of the most important classes of computer systems, yet they have received relatively little attention from many organizations” (Abaubkar, 2014).

If the security attached to the University's online databases is vulnerable, cyber-criminals could interfere with the databases and manipulate the systems without a trace. Such protection is needed to preserve the privacy of an individual in the institution and prevent abuse of the data stored.

Based on the preliminary investigation, the researcher observed that in Umaru Musa Yar'adua University, Katsina, students' academic records are usually stored in the database (web-based). There are several security measures put in place to safeguard the institutions' data. These include but are not limited to protection against SQL injection, data encryption, brute-force attack, and database redundancy. All these measures, though highly efficient in safeguarding any web-based data, still leave the institution's data vulnerable to phishing scams, social engineering, spyware, malware, and intruders.

Many tertiary institutions face the challenges of implementing cryptographic protection and information security measures to meet a wide range of requirements beyond regulatory compliance. Thus, unauthorized users could gain access to staff or student login details hence can access, modify and process such data without a mandate from the University authorities concerned. This is a big challenge that becomes imperative for this study.

Objectives of the Study

The objectives of this study are:

1. To examine the extent to which cryptography has prevented the security breach of electronic databases in UMYUK Katsina.
2. To identify the challenges encountered in the application of cryptography in UMYUK Katsina.

Literature Review

Security Breaches

In a world where data is everywhere, the need to protect vital information is essential. Complex, heterogeneous IT environments make data breach and threat response very difficult. The threat represents the type of action likely to be of harm (Kioskea, 2013). A threat is something that potentially violates security. It exists when there is a circumstance, capability, action, or event that could breach security and cause harm i.e., it is a possible danger that might exploit the vulnerability. According to Steve (2007), security breaches can be classified as unauthorized data observation, incorrect data modification, and data unavailability, which can lead to loss of confidentiality, availability, integrity, privacy, theft, and fraud. Similarly, Schneier (1997) postulated that the security threats to electronic databases include the following: viruses, spyware, Denial of Service (DOS) attacks, 8K, Distributed Denial of Service (DDOS) attacks,

buffer overflow attacks, brute force attacks, SQL injection, backup data exposure, database platform vulnerabilities, phishing scams, social engineering, and super-users with broad access rights.

Cryptography

In organizations where virtually all data of any importance is held on a computer system, the necessity of cryptography cannot be disputed. “When people started doing business online and needed to transfer funds electronically, cryptography applications for integrity began to surpass its use for secrecy. Hundreds of thousands of people interact electronically every day, whether through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The constant increase of information transmitted electronically has led to an increased reliance on cryptography and authentication” (Abubakr, 2014). “Cryptography is the art of combining some input data, called the plaintext, with a user-specified password to generate an encrypted output, called ciphertext, in such a way that, given the ciphertext, it is extremely difficult to recover the original plaintext without the encryption password in a reasonable amount of time” (Kremlin, 2008). According to Kayarkar (2012), modern cryptography prevents sensitive data from wrong hands in almost all kinds of attacks.

“Defenders must protect their system against any possible vulnerability, but an attacker need only find one security flaw to compromise the whole system. While no one can guarantee 100% security, cryptography can help significantly. The good news is that if an organization already has the algorithms and protocols, it can secure its systems; the bad news is that implementing the protocols successfully requires considerable expertise” (Schneier, 1997).

The popularization of the Internet has brought fundamental changes to the world because it allows a universal method of communication between computers. This carries enormous benefits with it but also raises many security considerations. “Cryptography is a fundamental technology used to provide security of computer networks, and there is currently a widespread engineering effort to incorporate cryptography into various aspects of the Internet. Most of the difficulty in engineering cryptographic systems has to do with understanding the trust relationships between different entities involved in a protocol” (Murphy and Badger, 1996). Security mechanisms that rely on cryptography are an integral part of almost any computer system in most organizations (Katz and Lindell, 2007).

Challenges to the Application of Cryptography

Data security and the challenges of data protection are increasing in scope and difficulty. While many organizations have long needed to safeguard intellectual property and confidential information, changes in information technology and business models introduce new actors, new threats, and new regulations.

As a result, organizations need to think beyond the traditional models of securing the perimeter and locking down specific segments of IT infrastructure to formulate their data protection goals. Schneider (2013) identified some inherent challenges to the application of cryptography include the following:

1. "Strength of encryption (algorithm, key size)"
2. "Quality of encryption (sufficiently reviewed by experts)."
3. "Implementations subjected to accreditation."
4. "Speed of encryption"
5. "Management of the persistent encryption keys"
6. "Randomness (use of random number generator) jargon"

The aforementioned must be implemented perfectly, or the system will fail. A poorly designed user interface can make a hard-drive encryption program completely insecure. Under deadline and budget pressures, implementers use bad random-number generators, do not check properly for error conditions, and leave secret information in swap files. Since such mistakes are not apparent in testing, they end up in finished products. More often than not, organizations fail to catch these subtleties and implement insecure algorithms and protocols. **McCurley (1996)** opined that "the challenges to the application of cryptography include: poorly designed user interface, quality of encryption (sufficiently reviewed by experts), scalable cryptographic primitives, management of the persistent encryption key, encryption can often be a computationally intensive process, randomness, use of bad random-number generator, lack of checking for error conditions leave secret information in swap files and speed of encryption among others." "Design work is the mainstay of the science of cryptography, and it's very specialized. Cryptography blends several areas of mathematics: number theory, complexity theory, information theory, probability theory, abstract algebra, and formal analysis. Few can do the science properly, and a little knowledge is a dangerous thing: Inexperienced cryptographers almost always design flawed systems. Nothing substitutes for extensive peer review and years of analysis" (Schneider, 2013).

Methodology

This study adopts a descriptive research design of Survey types. All the 21 staff members of the Directorate of ICT in UMYUK formed the population of the study. The data collected for this research were presented and analyzed using descriptive statistics and inferential statistics.

Findings and Discussions

The data collected and analyzed were presented and discussed as follows:

The extent of Cryptography Prevention of Security Breach of Databases in UMYUK.

The first objective of this research was to determine the extent to which cryptography has prevented security breaches of databases in UMYUK. To achieve this objective, the opinions of the respondents were rated using the five Points Likert Scale of Measurement in the following order: Very Large Extent, Large Extent, Extent, Undecided, and Not at all. However, for the researcher's convenience, the options were merged into 3 (Extent, Undecided, and not at all) to ease comprehension in the discussion, as depicted in Table 1.

Table 1: Extent of Cryptographic Prevention of Security Breaches of Electronic Databases in UMYUK

The table 1 depicts the responses of the respondents on the extent to which cryptography prevented security breaches in electronic databases in UMYUK. An observation of the table revealed that the majority of the respondents with the highest frequencies of over 55% average scores respectively indicated that cryptography had not prevented the occurrences of denial of service attacks (DOS), brute force attacks, SQL injection, back up data exposure, database platform vulnerabilities, social engineering and super users with broad access rights in the electronic databases of Umaru Musa Yar'adua University Katsina. This finding concords with that of Steve (2007) and Schneier (1997), who postulated that the security threats to electronic databases include the following: viruses, spyware, Denial of Service (DOS) attacks, brute force attacks, SQL injection, backup data exposure, database platform vulnerabilities, phishing scams, social engineering, and super-users with broad access rights among others.

The implication of this finding is that when security safeguards are not adequate, trespassers run little risk of getting caught. They can attack a system using techniques the designers never even considered. However, it can be seen that incorrect data modification 12 (60.0%), spyware, unauthorized data observation, and phishing scams with 10 (50.0%) scores each were the major security breaches that cryptography has prevented to a very large extent in UMYUK. Whereas 25.0% of the same respondents were undecided about the extent to which cryptography prevented the occurrence of virus, spyware, distributed denial of service attack, buffer overflow attack, and unauthorized data observation, respectively.

Challenges of Application of Cryptography in UMYUK

This research question was raised to identify the challenges encountered in the application of cryptography in UMYUK. In order to do this, a list of options containing different challenges in the application of cryptography was provided for the respondents to tick as many challenges as applicable. The table 2 provides a summary of the responses of the respondents.

Table 2: Challenges Encountered in the Application of Cryptography in UMYUK

Challenges in the Application of Cryptography	Yes		No	
	Freq.	%	Freq.	%
Poorly Designed User Interface	16	80.0	4	20.0
Quality of Encryption (sufficiently reviewed by experts)	17	85.0	3	15.0
Scalable Cryptographic Primitives	6	30.0	14	70.0
Management of the Persistent Encryption Key	5	25.0	15	75.0
Denial of Service Attacks	14	70.0	6	30.0
Computationally Intensive Process	16	80.0	4	20.0

Compliance Requirements and Auditors	11	55.0	9	45.0
Randomness	14	70.0	6	30.0
Use of Bad Random-Number Generator	11	55.0	9	45.0
Lack of Checking for Error Conditions Leave Secret Information in Swap Files	15	75.0	5	25.0
Speed of Encryption	18	90.0	2	10.0

The table 2 revealed that several challenges had affected the application of cryptography in electronic databases in Umaru Musa Yar'adua University Katsina (UMYUK). A cursory look at the table indicated that poorly designed user interface, quality of encryption(sufficiently reviewed by experts), denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions, and speed of encryption were the common challenges encountered in the application of cryptography with the highest frequencies of over 65% response scores respectively in UMYUK. This corroborates the earlier findings of **McCurley (1996) and Schneider (2013)**, who in their separate studies revealed that “poorly designed user interface, quality of encryption (sufficiently reviewed by experts), scalable cryptographic primitives, management of the persistent encryption key, encryption can often be a computationally intensive process, randomness among others were the challenges associated with the application of cryptography.

On the other hand, it was revealed that scalable cryptographic primitives and management of the persistent encryption key were the only 2 challenges not encountered in the application of cryptography with the highest frequencies of over 60% response scores.

Summary of the Major Findings of the Study

1. That cryptography has not prevented the occurrences of denial of service attacks (DOS), brute force attacks, SQL injection, backup data exposure, database platform vulnerabilities, social engineering, and super users with broad access rights with the highest frequencies of over 50% average scores respectively in UMYUK.
2. That poorly designed user interface, quality of encryption, denial of service attacks, computationally intensive process, randomness, lack of checking for error conditions, and speed of encryption were the common challenges encountered in the application of cryptography with the highest frequencies of over 65% response scores respectively in UMYUK.

Conclusion

From the analysis and summary of the findings of the study, it is clear that the Directorate of Information and Communication Technology of Umaru Musa Yar'adua University, Katsina, has realized the need for the application of cryptography as part of the defense-in-depth strategy

for providing reasonable protection of sensitive information vis-à-vis the means of detection and remediation of security breaches. However, the DICT does not explore, to a large extent, the advantages of security mechanisms opened in the application of cryptography for preventing the occurrences of most security breaches on the databases of the University.

Recommendations

1. The Directorate of Information and Communication Technology should, as a matter of policy, mount a regular training programme such as seminars, workshops, symposia, and in-house IT training for their staff to equip them with the latest development in the areas of information security systems to provide means of detection and remediation of security breaches of databases such as phishing scams and the like.
2. The need for employment of specialists in the areas of Information Security for safeguarding vital information in the Directorate of Information and Communication Technology is highly advocated as it would help the DICT staff to identify gaps that need to be closed in terms of challenges hindering the application of cryptography in UMYUK to cater for the database security breaches.

References

- Abubakar, A. (2014). Application of cryptography for information security in Umaru Musa Yar'adua University, Katsina.unpublished M.Sc. Thesis at Ahmadu Bello University, Zaria.
- Bagdanov, D.(2007). How to securely perform computation on secret shared data. MSc. Thesis: University of Tartu.
- Christian Kirsch –Thales (2009). The role of encryption in database security.Retrieved 14th January, 2014 from <http://www.net-security.org/insecure-archive.php>.
- Katz, J. and Lindell, Y (2007). Introduction to modern cryptography: Principles and protocols. Chapman & Hall/CRC, Boca Raton London New York.
- Kioskea (2013).Introduction to information technology security.Retrieved on May, 2013. From <http://www.facebook.com/pages/Kioskea/117422445065179>
- Kremlin (2008).Concept of cryptography. Retrieved 12th April, 2014.From <http://www.kremlinencrypt.com/concepts.htm>
- Maurer, U. (2004). The Role of cryptography in database security.Zurich, Switzerland: Springer.
- McCurley, K. S. (1996). Cryptography and the Internet: Lessons and challenges. Retrieved 24th March, 2014 from <http://www.mccurley.org/papers/asiacrypt96/>
- Menezes, A.J. Van Oorschot, P.C. And Vanstone, S.A. (1997).*Handbook of Applied Cryptography*. London: CRC Press.
- Miessler, D. (2013). An information security concepts primer.Retrieved on 9th May, 2021.From <http://creativecommons.org>.
- Mohammed, Z. (2012). Fifty years of library and information service in Ahmadu Bello University, Zaria. *A paper Ppresented at the symposium to mark the Ahmadu Bello University, Zaria 50th Anniversary Golden Jubilee Celebrations.*

- Murphy, S. and Badger, M. (1996). 'Digital signature protection of the OSPF routing protocol', [Proceedings of the 1996 symposium on network and distributed systems security](#), IEEE.
- SafeNet (2014). Data encryption solutions. Retrieved 24th March, 2021, from <http://www.securethebreach.com/>
- Savu, L. (2013). *Cryptography role in information security*. Romania: University of Bucharest.
- Schneider, L. (2013). Information Security - Learn about information security. Retrieved on 18th April, 2021 from <http://www.about.com/>.
- Schneier, B. (1997). Cryptography, security and the future. Retrieved 10th April, 2021. From <http://www.schneier.com/cryptography.html>.
- Steve, G. (2007). Databases for embedded systems. *embedded computing design* magazine. Retrieved on August 13, 2013 from <http://www.embedded-computing.com>