Cascaded Encryption Scheme (CES) for Robust Content Security Over Internet Networks

O.B. Longe, A.B.C Robert, S.C. Chiemeke, O.F.W. Onifade, C. Okpalugo & T. Olaseni.

Abstract **- In an age when information exchange has been made more mobile by the advent and advances in internet technology, information security is assuming a worrisome dimension. Hacking, phishing, eavesdropping, scamming and a host of other vices have become the order of the day on communication channels. This research addresses the problem of data security on multimedia systems by proposing a cascaded approach to text encryption while in transit. The objective is to protect message content over public network by hybridizing and combining encryption algorithms in a cascaded format in a single document thus making breaking the codes more difficult for intruders. To counter this threats, new security technologies are required that persistently protect content throughout its lifetime. Conditional Access Systems (CAS) has been used to protect content delivered over cables. In [16] we presented a technique for protecting digital content on passing through Internet intermediaries. This present effort proposes a methodology that divides messages to be encrypted into packets coded using different encryption algorithm. Annotation techniques are implemented as pointers to sections within the documents to aid decryption.**

Index Terms **- Cascaded, Annotation, Access, Encryption, Protection, Internet, Intermediaries.**

I. INTRODUCTION

Advancements in network technologies has propelled the transmission of data, multimedia and mixed media contents over open networks. The security issues inherent in these schemes are better imagined than real. 2 major techniques for maintaining security across different network as either storing sensitive data on a removable medium or encrypting data over transmission channels was identified in [9].

Manuscript Received March, 21, 2008.

O.B. Longe is of the Department of Computer Science University of Ibadan, Ibadan, Nigeria. +2348024071175-longeolumide@yahoo.com

A.B.C Robert (P.hD) lectures at the Department of Computer Science University of Ibadan, Ibadan, Nigeria

S.C. Chiemeke (P.hD) is with the Department of Computer Science University of Benin, Benin City, Nigeria

O.F.W. Onifade is with Laboratoire Lorrain de Recherche en Informatique et ses Application (LORIA) Campus Scientifique, B. P. 239, 54506 Vandoeuvre-Lès-Nancy, France

C. Okpalugo lectures at the Department of Computer Science , Benson Idahosa University, Benin City, Nigeria.

T. Olaseni is a postgraduate student at the Department of Computer Science, university of Ibadan, Ibadan, Nigeria.

Encryption as the "last line of defense" for data – at rest or data stored in a database[8]. The technology of encrypting data is known as Cryptology, it is composed of cryptography and cryptanalysis.

The categories of data that needs to be kept encrypted include Credit –card information, Social Security numbers, Private correspondence, Personal details, Sensitive company information, Bank- account information. In recent years according to [8], some consumer electronic devices, such as mobile phones, have also started to provide the function of saving and exchanging digital speech/music data, images and video clips under the support of multimedia messaging services over wireless networks, which is urgently demanding for multimedia security. Similarly, reliable security in storage and transmission of digital speech data, images and videos is needed in many real applications, such as Pay-Tv, Medical Imaging systems, military image database as well as confidential video conferences[13, 14].

Broadly, computer encryption systems belong to either the category of Symmetric (Private-key) or the Asymmetric (Public-key). Another classification of the encryption schemes are Deterministic / Probabilistic and Chaos based / Permutation only schemes, etc. Continuous development of these encryption algorithms (Cryptography) are equally been marched with examination and analysis of their strengths and weaknesses against known attacks such as the brute force attack, timing attack, session hijacking, replay attack, ciphertext-only , known-plaintext , chosen-plaintext attack and chosen-ciphertext [1, 15].

A. Encryption algorithms

Encryption algorithms are either symmetric or asymmetric. The symmetric encryption is also called private key or shared key encryption. Here, the encryption and decryption keys are identical and must be kept secret. Each pair of communicating partners or groups must have a secret key the same key is used for both encrypting and decrypting. Examples of symmetric algorithms include DES, AES, IDES, Blowfish and RC4. In a public key scheme, Asymmetric encryption, each individual has a pair of keys; a non-secret one for encrypting and a secret one for decrypting. The encryption key is known to anyone who wants it and is generally available from a well-known location to prevent spoofing. Because the encryption key is non-secret, anyone can encrypt a message for a particular recipient, but only the intended recipient has the

decryption key allowing the message to be read. Example of asymmetric encryption include: RSA, Diffie-Hellman , DSS, Elgammal, ECIIES and PGP. The strengths of asymmetric encryption are that they take care of the major problems of key distribution. Similarly, it is possible to provide authentication and non-repudiation. This is achieved by signing the message via a digital signature[2, 3,4].

Digital signatures work similarly, except that when X wants to sign a message to Y, X uses his/her private key Dx and computes Dx(m). Upon receipt, Y computes Ex(Dx(m)) = m. Since only X had knowledge of Dx, only X could have signed the message. Privacy encryption can be combined with digital signatures by computing Ey(Dx(m)), which is decrypted as Ex(Dy(Ey(Dx(m)))) = m.

The public key register of the Ei need not be read secure, since the Ei are given away freely. The registry must be protected against corruption, since that would allow fraudulent keys to be given out. The channel to the registry must be secure to prevent "spoofing" attacks, but this can be done using public key encryption.

Though, asymmetric encryption may work in securing data, but, the security could be lost if a public key is used to encrypt data for an entity that is not known. To enhance this, a certificate is required. A certificate authority (ACA) is a trusted third party which can issue a certificate (Providing the identity of an entity and its associated public key). Moreover, certificate provides a mechanism by which keys can expire and / or be revoked [3,4].

B. Multimedia encryption Schemes

Depending on the theories employed in the development of multimedia encryption schemes. Available multimedia encryption schemes include: Permutation – only encryption algorithms, Chaos-based schemes, Neural-network-based encryption schemes and Data security protection scheme for VOIP.

Chaos has good cryptography-like characters e.g. ergodicity, mixing and exactness, and sensitivity to initial conditions. On the basis of these, Chaos theory is employed by most encryption schemes as a mechanism to realize secret permutations of digital images / frames, or as a source to generate pseudo-random bits to control secret encryption operations.

The following are some Chaos related multimedia encryption schemes

- HCIE – Hierarchical Chaotic Image Encryption
- RCES - Recently Proposed Chaos- based Schemes
- MES – Multistage Encryption System
- DSEA – Semino Signal Encryption Algorithm
- TDCEA – Two Dimensional Circulation Encryption Algorithm
- NNBES – Nueral Network Encryption Schemes

According to [4], in image encryption, secret permutations are widely used to shuffle the positions of pixels (and/or pixel bits) which is an effective and easy way to make the cipher-image look “chaotic”. Similarly, in video encryption, secret permutations are widely used to shuffle the DCT/wavelet coefficients, blocks or macroblocks. The same idea has also been used in speech data encryption, by permuting the samples within each frame. There are many image/video/speech encryption algorithms that are based only on secret permutations which are called permutation-only (image/video/speech) ciphers. The main advantages of using only secret permutations in a cipher include easy implementation and the universality for most multimedia data formats.

C. Deterministic and Probabilistic Cryptography Schemes

Cryptography schemes can also be described as either being deterministic or probabilistic. The deterministic cryptography schemes are public key schemes in which for a fixed public key, the same plaintext will always encrypted to the same cipher text. With this scheme it will be very easy to se when one message is sent more than once. But it is problem encrypting a certain subset of message space. Examples of deterministic cryptography schemes include RSA, Diffie-Hellman , DSS, ECIIES and PGP [5,6,7].

Probabilistic Cryptography Schemes use random number every time a message is encrypted, hence a given plaintext may encrypt to different cipher text. This feature makes polynomially and semantically secure. Examples of Probabilistic Cryptography Schemes include Goldwasser-Micah, Blum-Goldwasser, Paillier Schemes, Darngard – Jurk Schemes, Elgamal and Elliptic Curve[6,15].

II. CONTENT PROTECTION OVER CABLES

Conditional Access Systems (CAS) popularly implemented using decoders Set Top Box (STB) were developed mainly to protect content delivered over cable and satellite networks and displayed on TV sets. In this technique contents are transmitted and delivered through a STB that is secured using Smart cards. The smart card, which is "owned" by the consumer is a Tamper-Resistant Device (TRD), as are some security-sensitive parts within the STB into which the smart card is inserted (e.g. the crypto modules). The STB stops functioning completely when the smart card is removed [17].

A. Implementing Protection Over Cables

In protecting contents over cable, the content is encrypted before being sent over the network and the encryption keys change frequently. At start-up, the network authenticates both the smart card and the STB hardware. When a client is interested in particular content, the client sends a request to the content provider who checks the request against a policy database. When the client is authorized to receive the content, the content is streamed and the correct decryption keys and key updates are sent over a secure connection initially set up between the content provider's server and the customer's smart card [16].

B. Content Protection Architecture

The architecture is based on a separate distribution chain for encrypted content on the one hand, and for usage rules and the decryption key on the other. Encrypted content together with a small amount of metadata is digitally signed and stored on a web download or streaming server. Metadata is descriptive data associated with the content. It may vary in depth from merely identifying the content title or providing descriptive information to populate an electronic program guide, to providing business roles detailing how the content may be displayed, copied, or sold. The framework is shown in Figure 1.

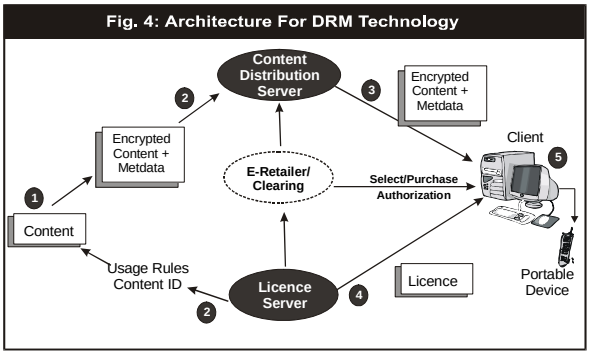


Fig.1: DRM Architecture for Content Management

C. Annotation

[10] viewed annotation from two perspectives. One point of view is to look at annotation as activity (action) and the other standpoint is the object annotation. The concerns in this work in primarily on the object annotation, though it may be necessary to make reference to the annotation in its active form from time to time. An annotation object is defined as an explicative note on a document to help in a specific interpretation of information contained in a document.

III. ENCRYPTION AND ANNOTATION

This conception can be demonstrated with example of opening an Internet sites with a browser. An internet site can be seen as a uniform document that must be interpreted by a browser. Each term (word) interpreted by the browser in the page can be referenced to another page (these references can be considered as annotation). It must be emphasized that each page referenced must be decoded with a particular scheme (example are browser, word, power point, PDF etc). Interpretation of a linked page is independent of the interpretation / decoding of other pages referenced in the document. Individual interpreted page is interpreted uniformly by an interpreter/decoding application.

An information source is divided into packets. Each packet can be encrypted by specific encryption rule. The rule guiding each of the packets is defined in an associated annotation anchored to that packet. An annotation anchored to a packet can again be linked to another annotation. When an annotation is attached to existing annotation, the source annotation is in turn regarded as a complete information source.

A summary of an information source was defined as

$$\Delta t.\sum \rho.\Psi.\Delta x.\mathrm{E}x$$

Where

Δt is a general summary of the entire information resource. It specifies the number of packet in the entire information source

ρ is referential location of specific information packet with reference to other packets in the entire information source. In a case where paragraphs are used for example, it may represent the paragraph number. In a more complex system, it may be meaningful to consider it as ordering position relative to the entire information source.

Ψ is series of codes or text information in that packet of interest

Λx is the annotation associated to that packet. An annotation is the explanation on how that packet should be rendered.

Ex is the encryption standard used on that packet. In normal textual information, it may be English, French, Chinese, etc.

A packet of a typical Internet web page can be described similarly as:

(message-location, associated message, URL linked, required browser)
A web page consulted at 09:28:15 UTC, Wednesday, September 05, 2007 was used as example

Figure 2: Webpage considered as packets for encryption

From the webpage above , a sub headline was used as an example as follows:

Information location : Google.com
Associated information : google news
Linked URL : http://news.google.com/nwshp?tab=wn
Browser : Mozilla firefox
Number of packets : twenty
e. A node was described as:
Packet number : two

With respect to the division of information sources into packets and subsequent possible subdivisions, each packet in an information source and the entire information source has specific node relative to the hierarchy information. Each node may or may not have a child node

$\rho = N(\mathrm{n}, \mathrm{P} \rightarrow m \leq 1, \mathrm{C} \rightarrow 0 \leq \mathrm{X} \geq \mathrm{n}).\theta$

Where

N is node point
P represents the parent. Typically P is either P(0) or P(1) representing whether it is a root or not respectively and
C are the number of children
n is the number of child sharing the same node
θ is the reference point to the node (example 1.3.3)
m is the number of parents sharing a node (0 or 1)

The concept of node associated with the packet location can give us a complete visual description of the relationship that exists within the packets in an information source.

Node has a parent and an array of independent children. A node may not have a parent (as in the source document). A node can not have more than one parent. It may not have implied or associated parent. A node may have other children occupying the same node. In the case of the source document, there is just one child and no parent. A child at a node may not necessarily share properties with another child on the same node or on any other node. A node may not have a child (a leaf), and a node must have finite number of children n.

A node and its annotation can be expressed as: $\rho\Lambda x$

where Λx are the annotations on a node and ρ is the node. It was assumed that a node may have more than one annotation. All annotation on a node are independent to one another in terms of context but are related in terms of their association to their common parent.

IV. MODELING/ EXPERIMENTS

An information source can be viewed as an array of annotations. The size of information in an array is dependent on the number of packets assigned to the entire information source. The essence of these annotations is to enable user encode or decode the information. The work assumed that, a section of the information can be extracted and decoded if the associated annotation is provided.

The entire information source is described as

$$\sum_0^n Pn\beta \bullet (\infty \ell \Phi d\alpha)$$

Where

Pn is the packet number. Packet 0 is the summary packet of set of information.
β is the code style for a given packet
∞ is the link for a given packet.
l is the location description
d is the content description associated to language or application of original content
α is the associated application required to interpret coded information

Annotations are referenced with packet labeling. Packet with number 0 was attributed to the summary annotation. The summary annotation describes the entire document in consideration. The attribute describing the content of information are not in textual form but coded as well.

A. Experiments

The news journal in Figure 2 was experimented with. Two hypothetic encryption methods were applied to different section of the news journal. Associated pages were also encrypted using these methodologies. The resulting annotations and code are shown below.

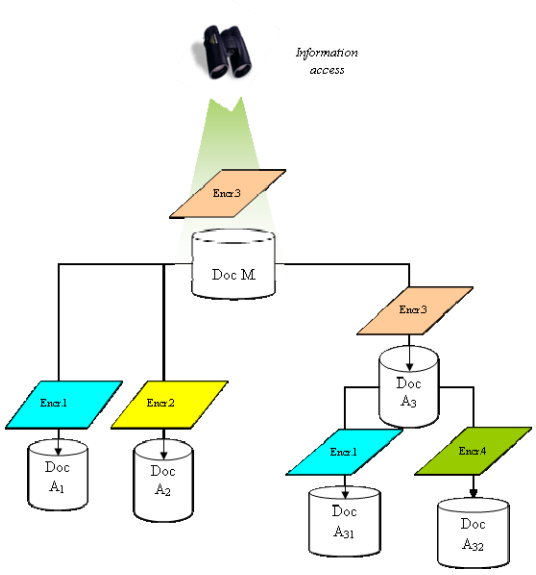


Figure 3: Layout of Cascaded Information Encryption

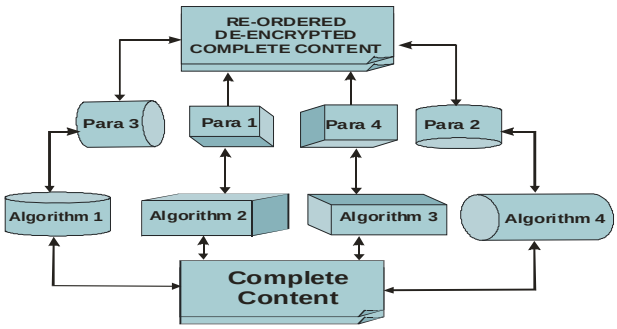
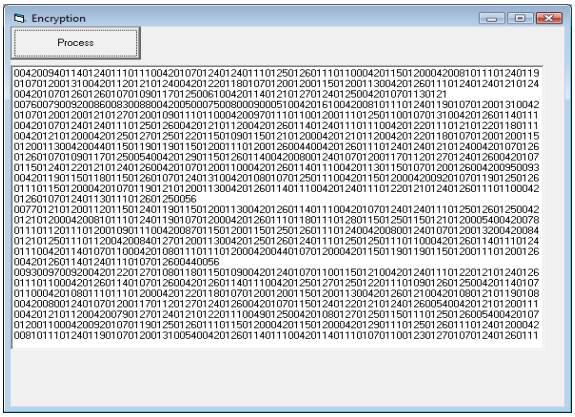


Figure 4: Layout of Cascaded Information Encryption



Figures 5: Encrypted page of news in packet 2 of figure 1

<packet1>
<packets>0</packets>
<codestyle>ascii+2-4</codestyle>
<link>http://member.lycos.co.uk/charlesrobert/news2.htm</link>
<datestamp>13h22 15-09-2007</datestamp>
<location>Node: section 2</location>
<information>2 terror suspects arrested in Germany</information>
<browser>Internet navigator </browser>
</packet0>

Figure 6: An annotation of a packet

V. CONCLUSION/FUTURE WORK DIRECTION

We have demonstrated the importance of using annotations to aid decryption when several encryption standards are hybridized for the protection of digital contents. This approach, a simplification of reality, van be extended to also protect other multimedia contents during transmission. Future direction will be to implement this framework and benchmark various hybridized algorithms to evaluate their and ability to withstand different hacking attacks.

REFERENCES

[1] J. Buchholz. “Matlab Implementation of the Advanced Encryption Standard” 2001, http://buchholz.hs-bremen.de

[2] M. Rogawski. ‘Analysis of Implementation of HIEROCRYPT–3 algorithm (and its comparison to CAMELLIA algorithm) using ALTERA devices. 2003. http://arxiv.org/ftp/cs/papers/0312/0312035.pdf

[3] J. Black, S. Halevi, H. Krawczyk, T. Krovetz and R. Phillip, "UMAC: Fast and Secure Message Authentication".. Advances in Cryptology - CRYPTO '99. Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 216-233.

[4] E. Biham and A. Shamir. “Differential cryptanalysis of DES-like cryptosystems” Journal of Cryptology, vol. 4 num. 1, pp. 3–72, Springer-Verlag, 1991 URL : http://www.springerlink.com/index/K54H077NP8714058.pdf

[5] D. Coppersmith. "The Data Encryption Standard (DES) and its strength against attacks" (PDF). IBM Journal of Research and Development 38 (3): 1994 p 243. http://www.research.ibm.com/journal/rd/383/coppersmith.pdf

[6] N. Ferguson and Schneier, D. " Cryptanalysis of Akelarre (attack on Akelarre)" Workshop on Selected Areas in Cryptography (SAC '97) Workshop Record, School of Computer Science, Carleton University, 1997, pp. 201--212.
[7] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden. "Quantum Cryptography, Reviews of modern physics" Volume 74, January 2002
[8] P. Erich and L. Siqing. "Using asymmetric encryption and digital signatures in a SQL server 2005 database" 4 Guys From Rolla February 28, 2007.
[9] L. Tyson. "Method for providing services in a data transmission network and associated components" URL http://www.freepatentsonline.com/y2007/0118749.html
[10] A.B.C. Robert: "KARIS: A multiple-scheme framework for encryption based on an annotation model for enhanced information security". Unpublished Manuscript. 2008.
[11] L. Tyson. "The Convergence of Physical and Information Security in the Context of Enterprise Risk Management. 2007 URL www.aesrm.org / www.isaca.org
[12] E. Moffaert. "Digital Rights Management" 2003. online at http://www.alcatel.com/document.
[13] O.B. Longe, O. B. "Software Protection and Copyright Issues in Contemporary Information Technology". Paper presented at the 2nd Annual Engineering Conference, Auchi Polytechnic, Auchi, Nigeria. August, 2004.
[14] O.B. Longe and S.C. Chiemeke. "The Design and Implementation of an E-Mail Encryptor for Combating Spam Mails from the Sending End". Proceedings of the International Conference of the International Institute for Mathematical and Computer Sciences. Covenant University, Ota Nigeria. June, 2006
[15] I. Renato. "Open Digital Rights Language (ODRL) Version 1.111". 2000. IPR Systems, Available online at http://www.w3.org/TR/odrl/
[16] S.C. Chiemeke and O.B. Longe. "Beyond Web Intermediaries: A Framework for Securing Digital Contents on Client Systems" Proceedings of the World Congress on Engineering(WCE) 2007. URL www.iaeng.org
[17] B. Schneier. "Applied Cryptography, Protocols, Algorithms and Source Code in C" Yorkshire; John Wiley Publishers. 1996.