ISSN:0975-9646

A Navel Approach to Identify Geo-Encryption with GPS and Different Parameters (Locations And Time)

V. Rajeswari[*1], V. Murali [*2], A.V.S. Anil[*3]

[*1] *Department of Research Programmes, CMJ University –Shillong, Meghalaya, India*

[*2,3] *Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool*

***ABSTRACT*- We are moving towards an era where location information will be necessary for access control. The use of location information can be used for enhancing the security of an application. Geo-encryption is the use of position navigation and time (PVT) information as means to enhance the security of a traditional cryptographic system. Geo-encryption builds on established cryptographic algorithms and protocols in a way that provide an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or board geographic area and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. In this paper we show how the traditional cryptographic system can be extended to incorporate the notion of location and other parameters (Time).**

Keywords: ***Geo-encryption, Location based security, GPS based encryption.***

I. INTRODUCTION

We are moving towards an age of ubiquitous computing where location information will be an integral part of many applications. Denning, MacDoran[1] and other researchers have described how the use of location information can make applications more secure. For instance, a user should be able to control or fire a missile from specific high security locations only. Verifying the location information in addition to the checks that are performed by traditional methods of authentication and access control will improve the security of the underlying application. Let's discriminate how location information can be used to augment traditional access control in order to cater to more sophisticated applications. Few examples will help to motivate our work. In a military application, if a computer containing top secret information is placed in a public place, then the computer should automatically become inaccessible. A critical application that is involved with the firing of missiles may have the following requirements: A user should be able to control or fire a missile from specific high security locations only. Moreover, the missile can be fired only when it is in a certain location. For such critical applications, we need additional checks, such as verification of the location of the user and the location of the missile, that must be satisfied before the user is granted access. Such checks based on location are not provided by the traditional access control models. The above examples illustrate how the use of location information can increase the security of an application geographically.

Traditional encryption is used to provide assurance that only authorized users can the secure content. However, it would still be useful to have an additional layer of security that provides assurance that the secure content can only be used at authorized location and time. The concept of location based encryption or Geo-encryption is being developed for such a purpose. The capability has tremendous potential benefits to applications such as managing classified/ secure data and digital movie distribution where controlling access is the predominate concern [2] .

To implement Geo-encryption, in principal, a device performing the decryption integrates a location sensor and cryptographic algorithms.

In this paper we propose a formal model for Geo-encryption. The paper describes how the Geo-encryption builds on conventional cryptographic algorithms and protocols and provides an additional layer of security. The paper then discusses the security analysis of the proposed scheme.

II. BACKGROUND

Before discussing Geo-encryption and its implementation, a review of some cryptographic terms, concepts and algorithms will prove useful.

A. Review on Cryptographic Concepts

The basic goal of most cryptographic system is to transmit some data, termed the plaintext, in such a way that is cannot be decoded by unauthorized agents. This is done by using a cryptographic key and algorithm to convert the plaintext into encrypted data or cipher text. Only authorized agents should be able to convert the cipher text back to the plaintext.

A cryptographic algorithm, also called cipher, is used to perform the transformation. The cipher is a mathematical function that used for encryption and decryption. There are two general types of key-based algorithms: symmetric and asymmetric (or public-key). Symmetric algorithms are the algorithms where encryption key can be calculated from decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are

the same as shown in Fig.1. These keys are often called session keys. Public-key algorithms are designed so that the keys used for encryption and decryption are different as shown in the Fig. 2. These keys cannot be mutually derived i.e. you cannot derive the decryption key from the encryption key. The encryption key is often called the public key and the decryption key is called the private key [3].

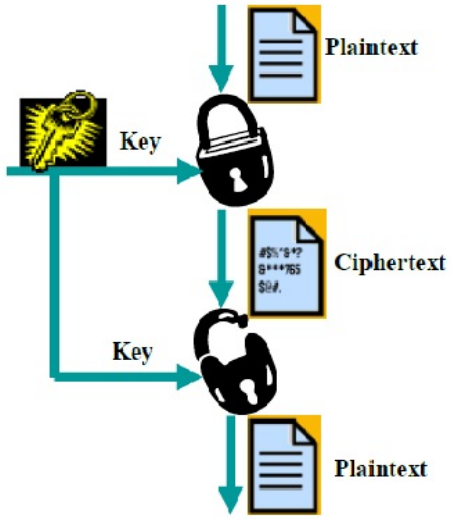

Fig. 1 Symmetric Algorithm

The most widely used symmetric algorithms are DES, Triple-DES and AES. The most popular public-key algorithm in use today is RSA, developed by Rivest, Shamir and Adleman[3]. AES and RSA will be used to implement our demonstration Geo-encryption protocol.

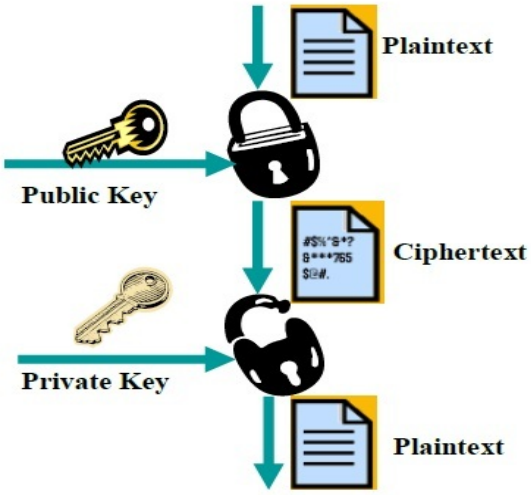

Fig. 2 Public-Key / Asymmetric Algorithm

There are two reasons why public-key algorithms are not used interchangeably with symmetric algorithm. First, public-key algorithms are slow, about 1000 times slower than the symmetric algorithms. Second, the public-key cryptosystems are vulnerable to chosen-plaintext attacks. Therefore, in most practical implementations, public-key algorithm is used for key management, to secure and distribute session keys. The plaintext is encrypted using symmetric algorithm. This is called a hybrid algorithm [3].

Authentication is another important concept in cryptography. It allows the receiver of a message to ascertain its origin. Authentication is not necessarily used in encryption or decryption protocols but it is a key concept in verifying the source of a message. It will be used for signal authentication. Hash functions are a fundamental building blocking for many of the authentication protocols. A hash function is a function that takes a variable length input and converts to a fixed length output, called hash value or hash digest [3]. Hash functions are relatively easy to compute but significantly harder to reverse. Beside one-way-ness, the other important property of hash functions is collision-free: It is hard to generate two inputs with the same hash value.

A Message Authentication Code (MAC) also known as data authentication code (DAC) is a one-way hash function with the addition of a key. The hash value is function of both of the input and the key [3]. Unlike encryption, authentication doesn't hide the plaintext but tag the MAC at the end of the plaintext for the recipient to verify whether the plaintext has been modified on the way of distribution.

III. A SCHEME TO STRENGTHEN THE SECURITY

In the location-based access control, it is extremely important to accurately determine the location of users and objects. There are different technologies for doing this such as GPS receiver or other satellite or Radio Frequency Positioning System.

The location of an object or user can be determined through GPS system. The object whose location was trying to determine must have a GPS receiver device which communicates with different satellite constellations to determine its location. The GPS covers a very wide area and the location information is accurate to within a few meters. Although the GPS was originally used only by military organizations, it is now being used by commercial organizations as well.

A. The Geo-Encryption Algorithm

In Principal, one could cryptographically bind or attach a set of location and time specifications to the Cipher text file and build devices that would decrypt the file only when the user is within the specified location and time constraints. However, this approach presents potential problems: the resultant file reveals the physical location of the intended recipient. The military frowns on this sort of things at least for their own forces. Furthermore, it provides vital information to someone who wants to spoof the device.

As another possibility, one could use location itself as the cryptographic key to an other strong encryption algorithm such as AES. This is ill advised in that location is unlikely to have sufficient entropy (that is uncertainty) to provide strong protection. Even if an adversary does not know the precise location, enough information may be available to enable a rapid brute-force attack analogous to a dictionary attack. For example, suppose that location is coded as a latitude-longitude pair at the precision of one centimetre and that an adversary is able to narrow the latitude and longitude to within a kilometre. Then there are only 100,000 possible values each for latitude and for longitude,

or 10 billion possible pairs (that is, keys). Testing each of these pairs would be easy.

Applying an obfuscation function to the location value before using it as a key could strengthen this approach. However, the function would have to be kept secret to prevent the adversary from doing the same. In general, security by obscurity is scoffed at because once the secret method is exposed, it becomes useless.

A guiding principal behind the development of cryptographic systems is that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public. But, that they are designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithms so that the best attack requires an exhaustive search of the key space and using sufficiently long keys that exhaustive search is infeasible.

The purpose of Geo-encryption is to provide security to the transmission of information. As such, it is important that every linkage of the Geo-encryption chain is secure. This includes not only the protocol itself but also the broadcast of RF signal. The basic protocol is discussed previously in [4]. The security of the RF navigation signal is provided by message authentication. Authentication is about the verifying the source of the data/messages. One goal is to prevent the user from being fooled into believing that a message comes from a particular source when this is not the case. Another goal is to allow the receivers to verify whether the messages have been modified during transmission.

The grid could just as well be based on the Military Grid Reference System or the Universal Transverse Mercator system. In fact, instead of a point, an area with any arbitrary shape could have been used. For example, the shape of the Disneyland theme park could map to a single Geokey value to permit successful decryption when the user is located in the theme park but not when outside.

B. Anti-spoof Receivers:

Most civil or non-military GPS receivers are trivially easy to spoof or fool into determining erroneous positions: Simply hook up one of the many excellent signal simulators available and the receiver will buy into whatever location and time values you want. This characteristic is why military receivers use the Y-code, which is an encrypted version of the P-code. Unless spoofers have access to the correct cryptographic keys and know how to generate Y-code from P-code, they can't spoof the military set. They may be able to jam it, but not spoof it. Civil sets can be made difficult to spoof through a series of hardening measures. These include a variety of signal checks:

- Use a jamming-to-noise power ratio (J/N) meter to check for above-normal energy levels.
- Monitor carrier-to-noise-density ratio (C/N0) for consistency or unexpected C/N0 given J/N.
- Monitor the phase difference between antenna elements (all signals shouldn't come from the same direction).
- Use "deep acquisition" to look for weak, real

Numerous navigation checks can also be instituted:

- Compare "watch time" with "signals time" (most signal generators can't synchronize with GPS time).
- Conduct continuity checks in time and position.
- Conduct consistency checks with other navigation sensors.
- Check for large residual errors, particularly in differential correction channel(s).
- Use receiver-autonomous integrity monitoring (RAIM)-type functions.

With careful attention to detail, civil sets do not have to be as vulnerable to spoofing as most of them are.

C. Relay Encryption:

Successive geo-encryption can be used to force data and/or keys to follow a specific geographical path before they can be decrypted. This strategy is achieved by applying multiple Geo-Locks at the origination node prior to transmittal. As each required node is traversed, one layer of Geolocking is removed, thus ensuring the desired path has been followed.

Relay encryption might be useful for applications that use regional distribution centres for the distribution of data supplied by producers.

In some applications, it may be desirable to know that a message has followed a particular route. A process similar to the route-forcing technique in which each traversed node in effect stamps the message with its location and time values.

IV. CONCLUSION

Geo-encryption is an approach to location-based encryption that builds on the conventional cryptographic algorithms and protocols. It allows data to be decrypted a specific place or broad geographic area, and supports constraints in time as well as in space. Depending on individual implementations or with proper implementation of signal authentication, it also can provide strong protection against location spoofing.

REFERENCE:

[1] Dorothy E. Denning and Peter F. MacDoran. Location-Based Authentication: Grounding Cyberspace for Better Security. In Proceedings of the Computer Fraud and Security, Elsevier Science Ltd, February1996.

[2] L. Scott, D. Denning, “Location Based Encryption & Its Role In Digital Cinema Distribution”, Proceedings of IONGPS/GNSS 2003, pp288-297.

[3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc. 1996.

[4] A. Perrig, R. Canetti, J.D. Tygar, D. Song, “The TESLA Broadcast Authentication Protocol”, CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13