Satellite Networks for Key Management

A.Koltuksuz
Izmir Institute of Technology, ahmetkoltuksuz@iyte.edu.tr
Dept. of Computer Engineering, Urla, Izmir, 35430 TURKEY

***Abstract*-The cryptographic key management center is the place where all the cryptographical protocols and related keys are in action. Traditionally the key management centers operate on the ground. However; with the satellites, it is possible to conceive a space based key management center. This paper underlines the pros and cons of having a satellite networks key management center.**

I. INTRODUCTION

The science of secrecy or better known as the cryptography is able to provide some solutions to some of the contemporary issues of a digital society. Although the issue of secrecy that traditionally has been dealt with cryptographic solutions has come to be understood as to be the issue of communication secrecy actually it is much broader subject that calls for the information integrity functions. Some of the information integrity functions are privacy (secrecy), integrity, authenticity, digital signing, identification, authorization, license and/or certification, witnessing (notarization), concurrence, liability, receipts, certification of origination and/or receipt, endorsement, access, validation, time of occurrence, voting, ownership, registration, approval/disapproval, digital-money and, non-repudiation [1]. However, the application of any given cryptographic solution to any of the aforementioned issues first and the foremost calls for a key management infrastructure. And, customarily the key management is done by the earth based stationary centers.

This paper will try to come up with an alternative satellite base solution and will discuss the pros and cons of the proposed scheme. The rest of this paper is organized as follows: In section II the cryptosystems will be structurally classified by their employed key(s). While the cryptographic key management center will be detailed in section III the section IV will introduce the concept of satellite networking based key management. The advantages and disadvantages of the satellite network based key management system will be discussed in sections V & VI consecutively. The conclusion is given in section VII.

II. CRYPTOGRAPHIC NOMENCLATURE

Based on the type and the number of keys plus the way the keys themselves utilized any given cryptosystem can be mainly classified into two categories. The symmetrical cryptosystems are those which utilize one single key that is used for the purposes of both enciphering and deciphering. Formally:

A cryptographic transformation T is a sequence of transformations

$$T = \left\{ T^{(n)} : 1 \le n \le \infty \right\} \tag{1}$$

$$T^{(n)} : \mathbb{Z}_{m,n} \rightarrow \mathbb{Z}_{m,n} \tag{2}$$

Where $T^{(n)}$ specifies how each plaintext $x \in \mathbb{Z}_{m,n}$ is replaced by a ciphertext $y \in \mathbb{Z}_{m,n}$. And, $\mathbb{Z}_{m,n}$ is the set of plaintext formed from letters of the alphabet in $\mathbb{Z}_m$ [2]. Therefore

$$E_{k_1}(P) = C \text{ and } D_{k_2}(C) = P \tag{3}$$

where E is an encryption function with an encryption key of k_1 on plaintext P to obtain the ciphertext of C. Likewise D is the decryption function with a decryption key of k_2 on ciphertext to recover the plaintext. Now, since $k_1=k_2$, (3) can be rewritten as

$$D_k = E_k^{-1} \tag{4}$$

Equation (4) clearly defines the symmetrical cryptosystems with their one private (secret) key specification [3]. If the keys that are associated with both processes of encryption and decryption are different than each other which means that there is one set of key for each cryptographic function then that cryptosystem is an asymmetrical one and, formally

$$k_1 \neq k_2 \text{ and } D_{k_2} \neq E_{k_1}^{-1} \tag{5}$$

The asymmetrical cryptosystems are founded in the complexity theory and have their roots in the different branches of mathematics such as the number theory, lattices and polynomials e.g. Table 1 outlines the most basic asymmetrical cryptosystems with their respective mathematical roots.

TABLE I
ASYMMETRICAL PROTOCOLS

Mathematics	Instance	Asymmetrical Protocol
Number Theory	Discrete Logarithm Problem (DLP)	1. Diffie-Hellman Key Exchange (DHKE) [4]. 2. El-Gamal Cryptosystem [5]. 3. Digital Signature Standard (DSS-DSA) [6].
	Factorization	RSA Cryptosystem [7]
Algebraic Geometry	Elliptic curves	1. Elliptic Curve Cryptosystem (ECC) [8]. 2. Key exchange: ECDH [9]. 3. Key exchange: ECMQV [9]. 4. Elliptic Curve Digital Signature Algorithm (ECDSA) [9]
Lattice Theory	Lattices & Polynomials	1. Lattice based cryptosystems [10]. 2. NTRU [11].

III. THE KEY MANAGEMENT CENTER

In either of those aforementioned cryptosystems one of the most crucially important aspects is the key management. Since the key management is the heart and soul of any contemporary cryptosystem management center the rest of this section will try to underline the structure & basic functions of the cryptographic key management center. Any given cryptographic key management center has two main branches: (i) the mathematics based software cryptographic protocols and, (ii) the key operations performed in according to these protocols. The hardware, data and of the personnel dimensions of the cryptographic key management center is out of scope for this paper. The protocols are as follows:

- Asymmetrical Protocols: RSA [7], ECC [8], Lattice [12], El-Gamal [5] for secrecy & authentication.
- Key Exchange Protocols: DHKE [4], ECDH [9], ECMQV [9] for session key management.
- Digital Signature (Integrity) Protocols: DSS (DSA), [6], ECDSA [9] algorithms.
- Protocols for Hashing: SHA1-SHA2 family [12].
- Certification Protocols: X509 v.3 [13]
- Symmetrical Protocols: DES [14], Triple DES, AES [17].

Some of the key operations as required by these above protocols are listed below

- Prime number generation and primality testing for asymmetrical key pairs.
- The generation of public and private keys for asymmetrical cryptosystems.
- The announcement of the key & domain parameters.
- The deletion, revocation, updating, logging and identification of key pairs.
- Offline one-time session key generation, distribution and revocation for symmetrical cryptosystems. And, all logging services so as not to utilize the same key sets in future operations.
- Online session key generation through DHKE-ECDH-ECMQV and the similar algorithms for the online processes.
- The export & import operations for the keys.
- The key recovery.
- The certification operations: Generation, deletion, revocation, verification, updating, and publishing of the digital signatures.
- Providing an infrastructure as well as higher level protocols for the mobile digital signatures (m-signing). Plus acting as the certificate authority for m-signing as well.

IV. SATELLITE NETWORKS IN KEY MANAGEMENT

Customarily the key management centers are ground based operations. However, with the advancements in technology we now have the opportunity of having multiple satellites working in networks. Also the cubesats and possibly even smaller sized satellites are now feasible. Thus conceiving a key management center within a satellite is now totally possible.

A satellite key management center basically comprises a master satellite plus server satellites. The aforementioned functions of the key management center are now distributed to server satellites thus enabling the master satellite for fulfilling the functions of controlling & coordinating, logging, reporting and of archiving. The server satellites on the other hand will be solely responsible of the generation and the other related duties of key management. The below figure 1 shows the structure and functions of such a satellite network key management center.

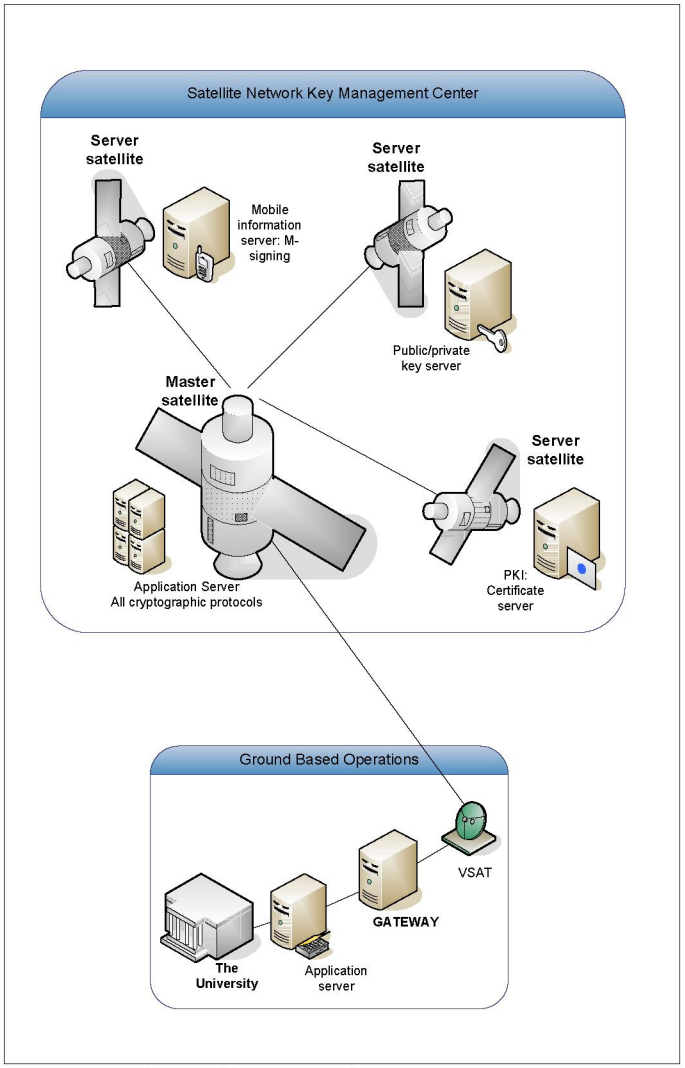

Fig.1 The Satellite Network Key Management Center.

The advantages of having a satellite network used as a distributed key management center instead of utilizing a ground based one are much higher. However; it is not without problems either. So the pros and cons of the Satellite Key Management Center can be summarized as follows:

V. THE ADVANTAGES of SATELLITE KEY MANAGEMENT CENTER

- Physically tamper proof.
- Very suitable for the mobile applications.
- Fast and reliable.
- Easy to reach from practically anywhere in the world.
- Very suitable for the cryptographic demands of the intelligence agencies.
- Cheap if and when cubesats-nanosats preferred.
- Distributed key management hence a backed up infrastructure plus enhanced reliability and security through distribution of the functions.

VI. THE DISADVANTAGES of SATELLITE KEY MANAGEMENT CENTER

- Expensive & hardness in maintenance if a conventional satellite networking preferred.
- National production is a prerequisite.
- Classical management problems of the distributed systems.

VII. CONCLUSION

A structurally new key management center is introduced in this paper. The proposed system is a satellite network deployed one hence a distributed key management center which is stationed in space.

REFERENCES

[1] G. J. Simmons, "Contemporary Cryptology," in Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons, Ed. New York: IEEE Press, 1992, pp. viii-xv.

[2] A.G. Konheim, Cryptography: A Primer, New York: John Wiley & Sons, 1981, pp. 13-28.

[3] A.H.Koltuksuz, "The Cryptanalytical Measures of Turkey Turkish for Symmetrical Cryptosystems,", unpublished Ph.D. thesis, Ege University, Turkey, 1995, pp. 26-29.

[4] W. Diffie, M. Hellmann, 1976, "New Directions in Cryptography," IEEE Trans. on Information Theory, 22, 1976, pp. 644-654.

[5] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Proceedings of CRYPTO 84 on Advances in cryptology, Santa Barbara, California, United States, 1985, pp. 10-18.

[6] NIST, National Institute of Standards and Technology, Digital Signature Standard, FIPS Publication 186-2, 2000.

[7] R. L. Rivest, A. Shamir, L. Adleman, "On Digital Signatures and Public Key Cryptosystems", MIT Laboratory for Computer Science Technical Memorandum 82, 1977.

[8] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation 48, USA, 1987, pp. 203-209. and, V. Miller, "Use of Elliptic Curves in Cryptography," in Lecture Notes in Computer Science, v. 218, London: Springer Verlag, 1985, pp. 417-426.

[9] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, New York: Springer-Verlag, 2004, pp. 172-184.

[10] D. Micciancio, S. Goldwasser, 2002, Complexity of Lattice Problems, A Cryptographic Perspective, The Netherland: Kluwer Academic Publishers, 2002, 216p.

[11] J. Hoffstein, J. Pipher, J. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem.", Springer: Lecture Notes in Computer Science v. 1423, 1998, pp. 267-288.

[12] NIST, National Institute of Standards and Technology, Secure Hash Standard, FIPS 180-2, 2002.

[13] International Telecommunication Union, ITU-T, X509, 1995.

[14] NIST, National Institute of Standards and Technology, Data Encryption Standard, DES, FIPS 46-3, 1999.

[15] NIST, National Institute of Standards and Technology, Specification for the Advanced Encryption System AES, FIPS 197, 2001.