A REVIEW ON SECURITY AND TRUST IN EFFICIENT CONTENT-CENTRIC NETWORK

Rajeev Goyal

Assistant Professor, Department of CSE, ASET,
Amity University Madhya Pradesh, Maharajpura Dang, Gwalior (MP)- India 474005

Abstract

The major issue for discussion is the architecture of future internet, which faces the Security and Trust issues. In information centric network the data become independent from its location, application, storage, and means of transportation, enabling inter-network caching and replication. Such improved networks are beneficial in efficiency, better scalability with respect to information, bandwidth demands and improving robustness in communication scenarios. This paper studied one name based scheme where it uses identity-based cryptography (IBC) algorithms. In this verification of the content's integrity, authenticity and flexible confidentiality protection are achieved. Also, one more approach which is the combination of traditional public-key infrastructure (PKI) and IBC as a hybrid scheme.

Keywords-Content Centric Network; Information Centric network; Identity-based cryptography

I. INTRODUCTION

In Information Centric Networks (ICN), named content count as a major class for content publishing, managing, requesting, or determined by its content name rather than its IP address. The ICN can be of Content-Centric Network (CCN) or Named Data Network (NDN). However, to fulfill the built-in security requirements, name-centric principal and access flexibility arises new challenges. For finding this solution where we see how to enable trust and ensure secure communication between content users and publishers of the network.

II. BASIC MECHANISMS FOR CONTENT INTEGRITY AND AUTHENTICATION

Named Data Network (NDN) and Content-Centric Network (CCN) introduced some basic mechanisms where content ought to have digitally signed. This sign is done by its publisher's private key which is verified later with the help of the publisher's public key at the time of receiving the data on the router. The major downside with content confidentiality is its content based authorized users. It is a very typical approach for secure key distribution based on public /private key pairs of users. Overall, a Certificate Authority (CA) is required to ensure with the public/private key infrastructure. But practically, it's quite not possible.

The major issue with the content network scenario is the high value of certificate management and user-level key for the several massive organizations that square measure incontinent or impossible for sharing of the same key among multiple devices.

As we tried to find a solution for the security issue which is based on the type of public-key cryptography called identity-based cryptography (IBC).In identity-based cryptography, a public identity acts as a public key. This public key is used for the verification of the digital signature. So, any data can be encrypted by a public key and decrypted by the private key. Thus, IBC eliminates the undoubting issue of certificate management in PKI, which is used to turn states where no need for obtaining and verifying any certificate throughout the transmission.

III. INTRODUCTION OF THE IBC ALGORITHM WITH ITS WORKING

For electronic communication, public key cryptography offers very good protection. In this, it uses paired keys with mathematically related codes used to encrypt and decrypt the message. There we use the public key which is difficult to use any other public key cryptography because on the one side recipient has to prepare with both public and private keys and on another sender should know the recipient's public key. Usually, the sender queries a Certificate Authority (CA) to retrieve the target recipient's public key. This particular problem has a promising solution named identity-based cryptography (IBC) or identity-based encryption (IBE). During the process of encryption, our target is also to reduce s the complexity of the process. For this purpose, we derive the public key from the user identity rather than from any Certificate from a Certificate Authority (CA) of the encryption process. Also, no pre-enrollment required. It enables postdating of messages for future decryption and also enables postdating of messages for future decryption.

3.1 IDENTITY-BASED ENCRYPTION

Identity-based encryption (IBE) is a type of public-key cryptography where a third-party server uses a simple identifier, such as an e-mail address. This identifier is used to generate a public key for encrypting and decrypting the electronic messages. This process is used to reduce the complexity of the encryption process. This Process greatly reduces the burden of users and administrators. An additional advantage of this process is message recipient doesn't need any advance preparation or any specialized software for the communication.

3.2 HIERARCHICAL IDENTITY-BASED ENCRYPTION

Hierarchical identity-based encryption is used as a private key generator (PKG). It is used as a generalization of IBE which organizes a hierarchy. Hierarchical IBE (HIBE) currently supports two types of applications. First is for forwarding Secure Encryption where users have to periodically update their private keys [20] and in the Second, Use of HIBE [19] for conversion the NNL broadcast encryption System into a public key broadcast system [20].

IV. OUR FOCUSED SCHEMES

4.1TRUST MANAGEMENT SCHEMES WITH IBS

Traditionally PKI-based trust management scheme is not associated with a certificate authority (CA) or multiple certificate authority with users. Some Internet Services or some personal identification relations are used to provide trust in between certificate authority and user. These things are used to enhance the trust of contents which are published with the help of link in between contents and identities. Integrity Rules are used to verify these links. We use two approaches to manage trust between users and the Certificate Authority (CA).

First Approach is used when the provider signed its contents with the help of IBS. Where consumer verifies this signature of the provider. If verification is positive, the consumer assures about the integrity and identity of the authenticated provider. This approach derives the trust in between provider and consumer. The second approach built the trust of the named object where it uses the identity of named or prefix of the contents. Some authorization mechanism is for the network during this approach. Where a dedicated name is given to only authorized publishers. The analysis says that this approach is more reasonable.

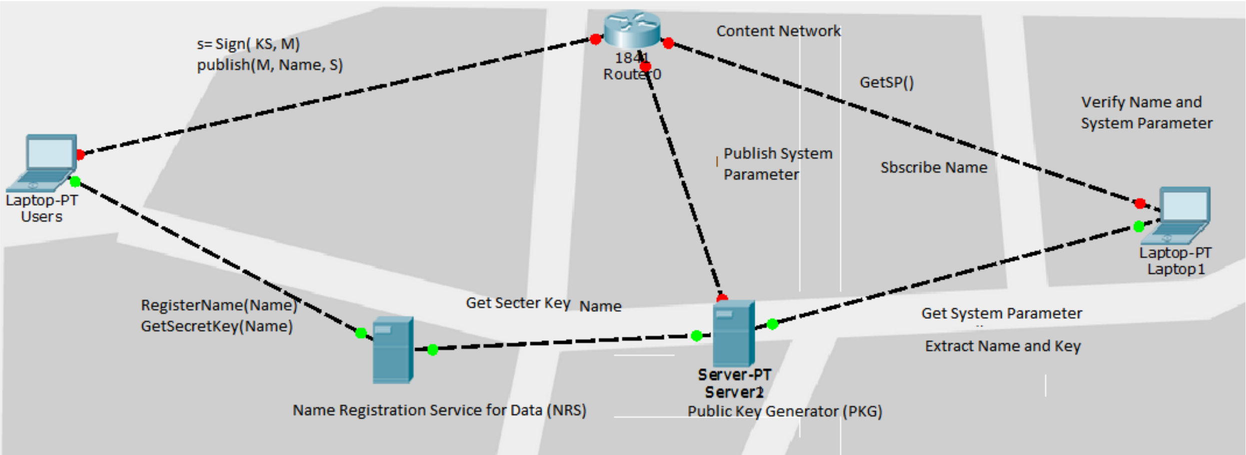

Figure-1 System Architecture

Figure-1 illustrates System Architecture which generates the system parameters (SP) and master secret key (MSK) based on the components of system architecture such as a private key generator, system parameter and master secret key. In this architecture view, PKG keeps the track of MSK and publish SP to the network. As we discussed that in the first approach firstly it obtains Secret Key (SK) with the identity of PKG. Extract Algorithm is used by PKG for generating the key for its identity and MSK. To obtain Secret Key (SK), we need some secure channel. After this process, SK is used to sign contents using Sign Algorithm. This is a one-time activity operation. We save the identity of the provider as metadata.

4.2. MAINTAIN CONFIDENTIALITY WITH THE HELP OF IBE

To send secret data with the help of IBE advanced features, the sender has no need to obtain any public key certificate of the receiver, which shows that IBE is more flexible for protection of data confidentiality. Especially in those situations where a content provider has no information's regarding the receiver's .that is why in advance there is no need to obtain a public key certificate. This is more useful in those cases where no reestablished secure communication channel is required. With the help of IBE, two approaches are used to maintain confidentiality. In the first approach, encrypting contents with the prefix or with its content name. Whereas the second approach encrypts the content with the identity of a receiver. Both approaches use Encrypt Algorithm to encrypt data with identities by Provider and Decrypt Algorithm uses by Receiver to obtain cleartext. Key Encapsulation Mechanism (KEM)is used to compute encryption and decryption cost, especially for huge contents. Also Data Encryption Key (DEK) for encrypting the contents.

4.3 A HYBRID APPROACH

As we see in Figure-2, we required a secure channel for distributing SK and the authentication channel to get SP of the PKG. We use some not scalable any offline handover or any pre-loading of a device or application for distributing Scathes all are known as out-of-band communication mechanisms. For this mechanism, we need to verify its authentication which ensures the belongings of a key to particular PKG domain or not. In this Hybrid Approach, PKI is deployed with the current Internet Infrastructure which makes this approach is more scalable. PKI-based trust infrastructure supports web-based Internet services such as server-side SSL/TLS, IPSec and DNSSEC.

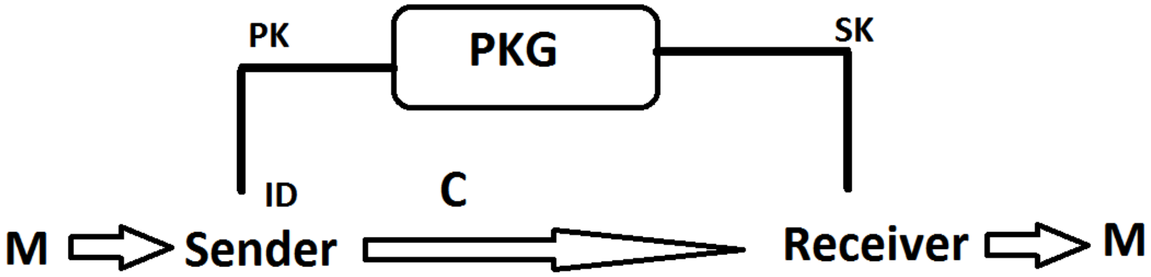

Figure-2 Typical IBC system

To get a scalable solution trusted parties CA certified domain ‘public keys as a form of evidence. After deep analysis, Researchers say that for domain level trust management PKI gives a feasible solution, which is fairly enough to get trust management for device and end-user. Benefits with the IBC such as name-based trust and security is not compromised in our Hybrid Approach. To verify the authenticity of a PKG’s SP, the consumer only requires domain ‘PK certificate. Working with this approach, trust is built on a content name or the identity of the content provider.

V. STUDY OF RELATED WORK AND FUTURE PLAN

Content Authentication Process for self-certifying given by Smatters and Jacobson [8] is basically a secure content mechanism. This mechanism ensures the integrity and authentication of the contents and names. To obtain security without providing extra efforts, bootstrapping security CCN [10] is used for demonstration, where we reuse the security-enhanced mechanism.

Our future plan is to achieve more security with the help of Content-Centric Network. For trust management specially used for contents, SPKI/SDSI is used by NDN with local namespaces. Trust Models used by PGP with the help of a trusted certificate. A certificate chain is obtained by a content consumer who verifies the authenticity of the content. This verification used to manage runtime performance and cost for mobile networks. ICN networks NetInf [7], PSIRP [11], and DONA [12] use hash of content or public keys for the identifiers and for verifications.

VI. CONCLUSION

To protect data in CCN and NDN, an identity-based signature and encryption mechanism has been proposed for optimizing integrity and trust. Our mechanism support bootstrapping content based trust. To enhance the scalability, the paper emphasizes on a hybrid approach which is the combination of PKI and IBC. There we draw a prototype of our solution with the help of CCNx and on Local Area Network (LAN); there we verified the effectiveness of confidentiality protection and integrity verification.

REFERENCES

[1] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. In Proc. of SIGCOMM, 2009.

[2] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In Proc. of ACM CCS, 2010.

[3] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In Proce. of CRYPTO, 2001.

[4] D. Boneh, E. Goh, and X. Boyen. Hierarchical identity-based encryption with constant size ciphertext. In Proc. of Euro crypt, LNCS 3493, 2005.

[5] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren. Secure naming for a network of information. In Proc. of IEEE Global Internet Symposium, 2010.

[6] F. Hess. Efficient identity-based signature schemes based on pairings. In Proc. of ACM SAC, 2002.

[7] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard. Networking named content. In Proc. of ACM CoNEXT, 2009.

[8] V. Jacobson, D. K. Smetterss, N. Briggs, M. Plass, and P. Stewart. Voccn: voice over content-centric networks. In Proc. of ACM Workshop on Re-architecting the Internet, 2009.

[9] P. Jokela, A. Zahemszky, S. Arianfar, P. Nikander, and C. Esteve. Lipsin: line speed publish/subscribe inter-networking. In Proc. of ACM SIGCOMM, 2009.

[10] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica. A data-oriented (and beyond) network architecture. In Proc. of ACM SIGCOMM, 2007.

[11] C. Schridde, M. Smith, and B. Freisleben. An identity-based key agreement protocol for the network layer. In Security and Cryptography for Networks, volume 5229 of LNCS, pages 409–422. 2008.

[12] A. Shamir. Identity-based cryptosystems and signature schemes. In Proc. of CRYPTO, 1985.

[13] D. K. Smetters and G. Durfee. Domain-based authentication of identitybased cryptosystems for secure email and IPSec. In Proc. of Usenix Security Symposium, 2003.

[14] D. K. Smetters and V. Jacobson. Securing network content. Technical report, PARC, 2009.

[15] M. Smith and et al. securing mobile phone calls with identity-based cryptography. In Advances in Information Security and Assurance, volume 5576 of LNCS, pages 210–222. 2009.

[16] L. Zhang and et al. Named data networking (ndn) project. Technical Report NDN-0001, PARC, 2010.

[17] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In J. Feigenbaum, editor, Proceedings of the Digital Rights Management Workshop 2002, volume 2696 of LNCS, pages 61–80. Springer, 2002.

[18] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In J. Kilian, editor, Proceedings of Crypto 2001, volume 2139 of LNCS, pages 41–62. Springer, 2001

[19] D. Boneh and X. Boyen. Efficient selective-ID identity-based encryption without random oracles. In C. Cachin and J. Camenisch, editors, Proceedings of Eurocrypt 2004, volume 3027 of LNCS, pages 223–38. Springer, 2004.

[20] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In E. Biham, editor, Proceedings of Eurocrypt 2003, volume 2656 of LNCS. Springer, 2003.