Volume 3, Issue 10, October 2018 ISSN (online): 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

HIBE Based Security for Content Distribution using Block Chains

Sheetal Khandelwal
Department of Information Technology
Zeal College of Engineering and Research, Pune

Dinesh Choudhari
Department of Information Technology
Zeal College of Engineering and Research, Pune

Nikita Gandhi
Department of Information Technology
Zeal College of Engineering and Research, Pune

Prof. Pranalini Joshi
Department of Information Technology
Zeal College of Engineering and Research, Pune

Abstract-:User content, and device names as a security primitive have been an attractive approach especially in the context of Information-Centric Networking (ICN) architectures. We leverage Hierarchical Identity Based Encryption (HIBE) to build (content) name-based security mechanisms used for securely distributing content. In contrast to similar approaches, in our system each user maintains his own Private Key Generator used for generating the master secret key and the public system parameters required by the HIBE algorithm. This way our system does not suffer from the key escrow problem, which is inherent in many similar solutions. In order to disseminate the system parameters of a content owner in a fully distributed way, we use block chains, a distributed, community managed, global list of transactions.

***Keywords*—**HIBE, Block Chain, Decentralized Network, Encrypt Data.

I. INTRODUCTION

Information-Centric Networking (ICN) is an emerging networking paradigm that has received attention recently by the research community. ICN architectures use content names as the main ingredient of their (inter-)networking functions. Therefore, it comes as a natural choice to consider content names1 as the basic security primitive for ICN. Using content names as the main building block of security mechanisms offers some intriguing advantages. Firstly, content names can be human readable, therefore, they can be memorable (as opposed for example to RSA public keys), thus it should be easier to disseminate them using out of band mechanism, e.g., by printing them on a business card, or including them in a slide presentation. Secondly, content names can be predictable, therefore, it could be easy to predict the name of a content item that has not yet been created, e.g., the name of the next chunk of a live video stream. Lastly, content names can be hierarchical, reflecting real world organization and business relationships.

In this paper we are concerned with content distribution in ICN networks (although our solution is generic enough and can also be used in other similar architectures). In particular, we consider the case in which a content owner wants to share content with some subscribers. We wish to provide content integrity protection and content provenance verification based on content names. Content integrity protection is an integral part of any content distribution system, since it assures that a (content) item has not been modified during transmission. In order to highlight the advantages of (content) name-based integrity protection consider the example of an item being made available (i.e., published) by several endpoints. Using legacy content integrity mechanisms, either all these endpoints should share the same public/private key pair, which raises security concerns, or a subscriber should learn the public key of the endpoint from which she received a (content) item. In our system all these entities would share some publicly available system parameters, as well as, a content-specific secret. A subscriber that knows the system parameters can verify a digital signature over the item no matter the providing endpoint. Content provenance verification allows a subscriber to verify that an endpoint that hosts some content has been authorized by the content owner to do so. This property, which is implemented using a controlled content storage delegation algorithm, is useful in cases where a subscriber wants to receive an

item only from endpoints trusted by the content owner, e.g., for accounting reasons, spam prevention, phishing protection, etc. Our work here does not aim to provide content confidentiality and access control, nevertheless, content confidentiality and access control solutions can be easily used in conjunction with our approach and system. Content storage delegation provides a secure way for a content owner to authorize a third party to host the content.

II. RELATED WORK

1) Hierarchical Identity-based Encryption

An Identity Based Encryption (IBE) scheme is a public key encryption scheme in which an identity (or a name, i.e., an arbitrary string) can be used as a public key. An IBE scheme is specified by the four algorithms, Setup, Extract, Encrypt and Decrypt, summarized as follows:

• Setup is executed by a Private Key Generator (PKG).

It takes as input a security parameter k and returns a master-secret key (MSK) and some system parameters (SP). The MSK is kept secret by the PKG, whereas the SP are made publicly available.

• Extract is executed by a PKG. It takes as input SP, MSK, and an identity ID, and returns a secret key SKID.

• Encrypt takes as input an identity ID, a message M, and SP, and returns a ciphertext CID.

• Decrypt takes as input CID, the corresponding private decryption key SKID, and returns the message M HIBE schemes consider hierarchical identities and specify an additional algorithm, Delegate:

• Delegate takes as input SP, SKID1 , and an identity ID1.ID2 and outputs SKID1.ID2

The Delegate algorithm is of particular importance as it enables the owner of an identity A to generate SKs for other identities that use A as a prefix, without communicating with the PKG. Fig. 1 illustrates the HIBE algorithms.

2) Block chains

A blockchain is a distributed ledger of transactions maintained by a network of trustless nodes. Each block of the blockchain contains a list of transactions organized in a Merkle tree. New blocks are added to the blockchain by the miners. The addition of a new block involves the computation of a solution to a computationally intensive puzzle. The miner that successfully solves the puzzle floods the block in the network: if this block becomes accepted by at least 51% of
the miners, then it is added in the blockchain. Miners have incentives (usually monetary) to calculate a valid block. Any network node can participate in the network of miners. The most well known blockchain is the one used by the Bitcoin crypto currency.3 Blockchains are often referred to as a democratic way of maintaining transactions as they rely on consensus for confirming transactions and require no central authority.

III. LITERATURE SURVEY

1) Naming in Content-Oriented Architectures
year: 2011
Author : Ali Ghodsi UC Berkeley alig@eecs.berkeley.edu

There have been several recent proposals for content-oriented network architectures whose underlying mechanisms are surprisingly similar in spirit, but which differ in many details. In this paper we step back from the mechanistic details and focus only on the area where these approaches have a fundamental difference: naming. In particular, some designs adopt a hierarchical, human readable names, whereas others use self-certifying names. When discussing a network architecture, three of the most important requirements are security, scalability, and flexibility. In this paper we examine the two different naming approaches in terms of these three basic goals.

2) *Unbounded HIBE and Attribute-Based Encryption:-*
Year: 2016
Author: Mansi Shinde, Sonali Ghorpade

We present HIBE and ABE schemes which are “unbounded” in the sense that the public parameters do not impose additional limitations on the functionality of the systems. In all previous constructions of HIBE in the standard model, a maximum hierarchy depth had to be fixed at setup. In all previous constructions of ABE in the standard model, either a small universe size or a bound on the size of attribute sets had to be fixed at setup. Our constructions avoid these limitations. We use a nested dual system encryption argument to prove full security for our HIBE scheme and selective security for our ABE scheme, both in the standard model and relying on static assumptions.

3) *CCNKRS: A Key Resolution Service for CCN*
Year : 2014

Author : Priya Mahadevan1 Ersin Uzun1 Spencer Sevilla2 J. J. Garcia-Luna-Aceves.

A key feature of the Content Centric Networking (CCN) architecture is the requirement for each piece of content to be individually signed by its publisher. Thus, CCN should, in principle, be immune to distributing fake content. However, in practice, the network cannot easily detect and drop
fake content as the trust context (i.e., the public keys that need to be trusted for verifying the content signature) is an application-dependent concept. CCN provides mechanisms for consumers to request a piece of content restricted by its signer's public key or the cryptographic digest of the content object to avoid receiving fake content. However, it does not provide any mechanisms to learn this critical information prior to requesting the content.

IV. PROPOSED SYSTEM

This paper defines mechanisms that take advantage of Hierarchical Identity Based Encryption (HIBE). HIBE is a public key encryption scheme in which an identity can be used as a public key. Our system uses content names as HIBE public keys. HIBE specifies an entity, namely the Private Key Generator (PKG), which generates the private keys that correspond to each identity. All HIBE algorithms require as input some publicly available System Parameters, SP, which are PKG specific. A single system-wide PKG results in a key escrow problem, since the PKG knows all private keys, whereas multiple PKGs would require a resolution mechanism that maps identities to SP. In our system we consider one PKG per content owner, eliminating this way the key escrow problem, and we use a blockchain to disseminate SP. Blockchains are data structures that securely record transactions and are maintained by a distributed network of trustless nodes. Our implementation uses the blockchain provided by Namecoin2, an open source information registration and transfer system based on the Bitcoin crypto currency.

Modules

A. File Upload/Download
B. Key Generator
C. Signature Generator
D. Block Chain Model
E. Network Model
F. Decryption Algorithm
G. Hashing Algorithm

System Overview:

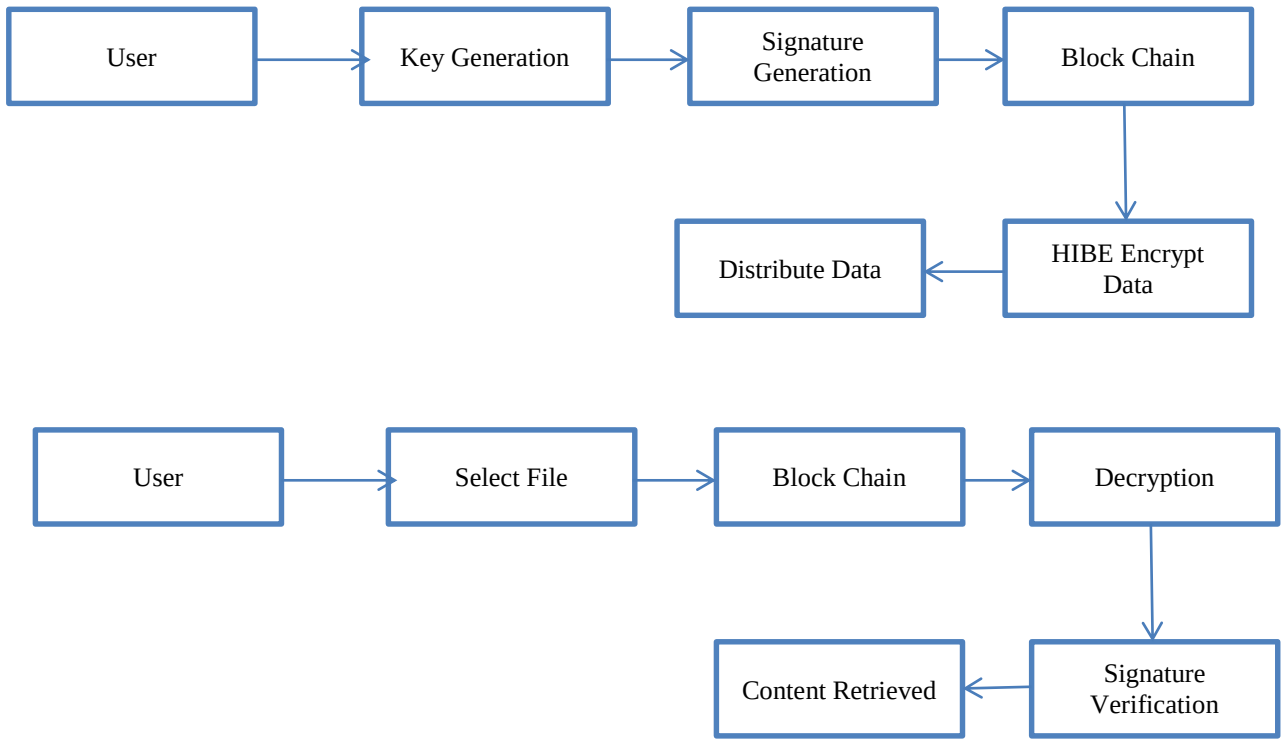

Fig-:1-System Architecture

CONCLUSION AND FUTURE WORK

We presented decentralized name-based security mechanisms that aim to secure content distribution in ICN and similar architectures. Our mechanisms leverage Hierarchical Identity Based Encryption (HIBE) to provide content storage delegation, content provenance verification, and content integrity protection. Our solution does not suffer from the key escrow problem, which is inherent in many other designs. Moreover, our solution uses blockchains to deliver the Systems Parameters, SP. Blockchains do not rely on any central authority, or on pre-trusted nodes, and provide interesting security properties. Our scheme is generic enough and can be incorporated into various ICN architectures, or any other similar system. In our prototype implementation we used separate, IP based, software, provided by Namecoin, in order to interact with the blockchain. Future work in this area could include the investigation of an ICN based blockchain implementation. Moreover, in our implementation we used the Lewko-Waters HIBE scheme. The advantage of this scheme is that it allows identifier hierarchies of arbitrary depth with constant-size SP. However, this comes at the cost of having SP with size larger than the size supported by the corresponding field of Namecoin, which we used. In order to solve this problem, either alternative blockchain implementations, or alternative HIBE schemes could be explored in the future.

References

1. G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A Survey of Information-Centric Networking Research," IEEE Communications Surveys and Tutorials, vol. 16, no. 2, pp. 1024–1049, 2014.
2. A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in Content-oriented Architectures," in Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking, ser. ICN '11. ACM, August 2011.
3. N. Fotiou and G. C. Polyzos, "Enabling NAME-Based Security and Trust," in Trust Management IX, ser. IFIP Advances in Information and Communication Technology, C. D. Jensen, S. Marsh, T. Dimitrakos, and Y. Murayama, Eds. Springer International Publishing, 2015, vol. 454, pp. 47–59.
4. A. Lewko and B. Waters, "Unbounded HIBE and Attribute-Based Encryption," in Advances in Cryptology - EUROCRYPT 2011, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, vol. 6632, pp. 547–567.
5. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Advances in Cryptology - CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin Heidelberg, 2001, vol. 2139, pp. 213–229.
6. A. Lewko, "Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting," in Advances in Cryptology EUROCRYPT 2012, ser. Lecture Notes in Computer Science, D. Point cheval and T. Johansson, Eds. Springer Berlin Heidelberg, 2012, vol. 7237, pp. 318–335.
7. J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 111–128, 2013.
8. Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, "Analysis of the HTTPS certificate ecosystem," in Proceedings of the 2013 Internet Measurement Conference, ser. IMC '13. New York, NY, USA: ACM, 2013, pp. 291–304.
9. D. Smetters and V. Jacobson, "Securing Network Content," PARC, Tech. Rep., 2009.
10. X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi, and G. Wang, "Towards name-based trust and security for content-centric network," in Network Protocols (ICNP), 2011 19th IEEE International Conference on, October 2011, pp. 1–6.
11. F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in Selected Areas in Cryptography, ser. Lecture Notes in Computer Science, K. Nyberg and H. Heys, Eds. Springer Berlin Heidelberg, 2003, vol. 2595, pp. 310–324.
12. V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," in Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, ser. CoNEXT '09. New York, NY, USA: ACM, 2009, pp. 1–12.
13. P. Mahadevan, E. Uzun, S. Sevilla, and J. Garcia-Luna-Aceves, "CCNKRS: A Key Resolution Service for CCN," in Proceedings of the 1st International Conference on Information-Centric Networking, ser. ICN'14. New York, NY, USA: ACM, 2014, pp. 97–106.
14. Y. Yu, A. Afanasyev, D. Clark, k. claffy, V. Jacobson, and L. Zhang, "Schematizing Trust in Named Data Networking," in Proceedings of the 2nd International Conference on Information-Centric Networking, ser. ICN '15. New York, NY, USA: ACM, 2015, pp. 177–186.
15. J. Kuriharay, E. Uzun, and C. Wood, "An encryption-based access control framework for content-centric networking," in IFIP Networking Conference (IFIP Networking), 2015, May 2015, pp. 1–9.
16. C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, "Interest-Based Access Control for Content Centric Networks," in Proceedings of the 2Nd International Conference on Information-Centric Networking, ser. ICN'15. New York, NY, USA: ACM, 2015, pp. 147–156.

17. M. Mangili, F. Martignon, and S. Parabosch, "A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in Content-Centric Networks ," Computer Networks, vol. 76, pp. 126–145, 2015.
18. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," IETF, RFC 4033, 2005.