Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 4 (2016) 17 - 22. Submitted 29/10/2016. Published 12/11/2016

GENERATING SEARCHABLE PUBLIC-KEY CIPHERTEXTS WITH HIDDEN STRUCTURES FOR FAST KEYWORD SEARCH

[1]Suganya.G, [2]Parameswari.V,
[1] M.Phil Scholar, Department of Computer Science, Bharathiyar Arts and Science College for Women's, Deviyakurichi, Salem,
[2]Assistant Professor, Department of Computer Science, Bharathiyar Arts and Science College for Women's, Deviyakurichi, Salem.

Abstract

Existing semantically secure public-key searchable encryption schemes take search time linear with the total number of the cipher texts. This makes retrieval from large-scale databases prohibitive. To alleviate this problem, this paper proposes Searchable Public-Key Ciphertexts with Hidden Structures (SPCHS) for keyword search as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable ciphertexts are structured by hidden relations, and with the search trapdoor corresponding to a keyword, the minimum information of the relations is disclosed to a search algorithm as the guidance to find all matching cipher texts efficiently. We construct a SPCHS scheme from scratch in which the cipher texts have a hidden star-like structure. We prove our scheme to be semantically secure in the Random Oracle (RO) model. The search complexity of our scheme is dependent on the actual number of the cipher texts containing the queried keyword, rather than the number of all cipher texts. Finally, we present a generic SPCHS construction from anonymous identity-based encryption and collision-free full-identity malleable Identity-Based Key Encapsulation Mechanism (IBKEM) with anonymity. We illustrate two collision-free full-identity malleable IBKEM instances, which are semantically secure and anonymous, respectively, in the RO and standard models. The latter instance enables us to construct an SPCHS scheme with semantic security in the standard model.

Keywords : SPCHS, Ciphertexts, Random Oracle.

1. INTRODUCTION

Network security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network Security concepts

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' also used (e.g., a fingerprint or retinal scan).Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Communication between two hosts using a network may be encrypted to maintain privacy.Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

2. RELATED WORK

Public-Key Encryption With Keyword Search (Peks)

PUBLIC-KEY encryption with keyword search (PEKS), introduced by Boneh et al.in, has the advantage that anyone who knows the receiver’s public key can upload keyword-searchable ciphertexts to a server. The receiver can delegate the keyword search to the server. More specifically, each sender separately encrypts a file and its extracted keywords and sends the resulting ciphertexts to a server; when the receiver wants to retrieve the files containing a specific keyword, he delegates a keyword search trapdoor to the server; the server finds the encrypted files containing the queried keyword without knowing the original files or the keyword itself, and returns the corresponding encrypted files to the receiver; finally, the receiver decrypts these encrypted files 1. The authors of PEKS also presented semantic security against chosen keyword attacks (SS-CKA) in the sense that the server cannot distinguish the cipher texts of the keywords of its choice before observing the corresponding keyword search trapdoors. It seems an appropriate security notion, especially if the keyword space has no high min-entropy. Existing

semantically secure PEKS schemes take search time linear with the total number of all ciphertexts. This makes retrieval from large-scale databases prohibitive. Therefore, more efficient search performance is crucial for practically deploying PEKS schemes. One of the prominent works to accelerate the search over encrypted keywords in the public-key setting is deterministic encryption focus on enabling search over encrypted keywords to be as efficient as the search for unencrypted keywords, such that a ciphertext containing a given keyword can be retrieved in time complexity logarithmic in the total number of all ciphertexts. This is reasonable because the encrypted keywords can form a tree-like structure when stored according to their binary values. However, deterministic encryption has two inherent limitations. First, keyword privacy can be guaranteed only for keywords that are a priori hard-to-guess by the adversary (i.e., keywords with high min entropy to the adversary); second, certain information of a message leaks inevitably via the ciphertext of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special scenarios.

3. EXISTING SYSTEM

One of the prominent works to accelerate the search over encrypted keywords in the public-key setting is deterministic encryption.An encryption scheme is deterministic if the encryption algorithm is deterministic. Focus on enabling search over encrypted keywords to be as efficient as the search for unencrypted keywords, such that a ciphertext containing a given keyword can be retrieved in time complexity logarithmic in the total number of all ciphertexts. This is reasonable because the encrypted keywords can form a tree-like structure when stored according to their binary values.Search on encrypted data has been extensively investigated in recent years. From a cryptographic perspective, the existing works fall into two categories, i.e., symmetric searchable encryption and public-key searchable encryption.

Disadvantages

- Existing semantically secure PEKS schemes take search time linear with the total number of all cipher texts. This makes retrieval from large-scale databases prohibitive. Therefore, more efficient search performance is crucial for practically deploying PEKS schemes.
- Deterministic encryption has two inherent limitations. First, keyword privacy can be guaranteed only for keywords that are a priori hard to guess by the adversary (i.e., keywords with high min-entropy to the adversary); second, certain information of a message leaks inevitably via the ciphertext of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special scenarios.
- The linear search complexity of existing schemes is the major obstacle to their adoption.

4. PROPOSED SYSTEM

This Project is interested in providing highly efficient search performance without sacrificing semantic security in PEKS. That starts by formally defining the concept of Searchable Public-key Ciphertexts with Hidden Structures (SPCHS) and its semantic security. In this new concept, keyword searchable ciphertexts with their hidden structures can be generated in the public key setting; with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching ciphertexts. Semantic security is defined for both the keywords and the hidden structures. It is worth noting that this new concept and its semantic security are suitable for keyword-searchable ciphertexts with any kind of hidden

structures. In contrast, the concept of traditional PEKS does not contain any hidden structure among the PEKS ciphertexts; correspondingly, its semantic security is only defined for the keywords.

Advantages

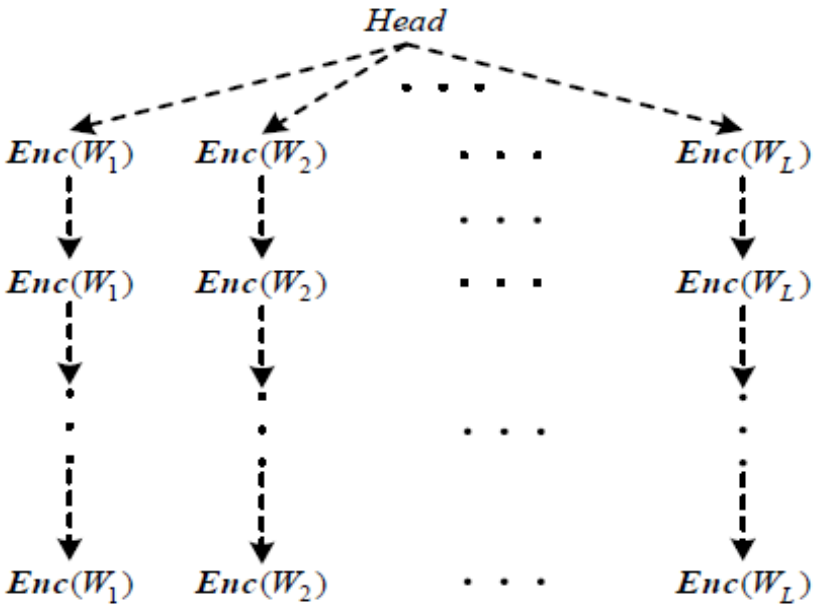
- We build a generic SPCHS construction with Identity-Based Encryption (IBE) and collision-free full-identity malleable IBKEM.
- The resulting SPCHS can generate keyword-searchable ciphertexts with a hidden star-like structure. Moreover, if both the underlying IBKEM and IBE have semantic security and anonymity (i.e. the privacy of receivers' identities), the resulting SPCHS is semantically secure.

Proposed System Algorithms

The encryption algorithm has two functionalities.

- search algorithm.
- Algorithm Trapdoor allows the receiver to delegate a keyword search trapdoor to the server.
- StructuredEncryption

System Architecture



We construct a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search.

5. SYSTEM MODEL

- **Login Module**
- **Trusted System Module**
- **Cryptography**
  - **Encryption**
  - **Decryption**
- **Sending Module**
- **Receiving Module**

Login Module

User gives the required username and password and then logins. If the login name and password in correct then he goes to the next form else he is asked to give the correct username and password.

Trusted System Module

Any trusted computer defines a clear trust boundary. For example, for a single chip ScP all components inside the chip may fall under such a trust boundary. Enforcing the trust boundary is by proactive measures for protection of components within the boundary. However, the regions inside a trust boundary that are physically protected can change dynamically, depending on the state of the ScP. when the CPU is off, there is no need to extend protection to all regions. However, when the CPU is on, the scope of protection will need to be wider.

CryptographyEncryption

I this module, we investigate the suitability of DOWN for identity-based encryption (IBE) and signature (IBS) schemes. We then motivate the need for low complexity ID-based authentication schemes for ScPs for evolving application scenarios. This includes an overview of some existing low-complexity ID-based KPS

Decryption

In this module a private exponent d is used for decryption and signing. More specifically, the private exponent needs to be stored in RAM for performing computations like decryption and signing.Modular exponentiation is often performed using the square-and-multiply algorithm.

Sending Module

In this module, the encrypted file is sent to the non-trusted system with the key, normal file is sent to the trusted system and also read only files are sent while sending the files details about the file and the path of the file is stored in data base. Before sending the file to the trusted and non-trusted systems we have to make sure that the server is made to run so that it can receive files from the client.

ReceivingModule

In this module the files are received. If it's a trusted system then the files receives without decryption else it receives in encryption mode with a secret key to decrypt the encrypt file and view the file. The files are usually stored in the path "c:\receive". If it's a read only file the user cannot edit or modify the file.

INPUT/OUTPUT

The input will be choosing trusted system and selecting IP address of both the trusted and non-trusted systems if there is no stored IP then new IP address will be entered and the output will be IP address gets stored in database and direct us to the main form.

CONCLUSION

This paper investigated as-fast-as-possible search in PEKS with semantic security. We proposed the concept of SPCHS as a variant of PEKS. The new concept allows keyword-searchable ciphertexts to be generated with a hidden structure. Given a keyword search trapdoor, the search algorithm of SPCHS can disclose part of this hidden structure for guidance on finding out the ciphertexts of the queried keyword. Semantic security of SPCHS captures the privacy of the keywords and the invisibility of the hidden structures. We proposed an SPCHS scheme from scratch with semantic security in the RO model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure. It has search complexity mainly linear with the exact number of the ciphertexts containing the queried keyword. It outperforms existing PEKS schemes with semantic security, whose search complexity is linear with the number of all ciphertexts. We identified several interesting properties, i.e., collision-freeness and full-identity malleability in some IBKEM instances, and formalizedthese properties to build a generic SPCHS construction. We illustrated two collision-free full-identity malleable IBKEM instances, which are respectively secure in the RO and standard models.

REFERENCES

[1] Boneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: PublicKey Encryption with Keyword Search. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004)

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238. Springer, Heidelberg (2004)

[4] Boyen X., Waters B. R.: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In: Dwork C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290-307. Springer, Heidelberg (2006)

[5] Gentry C.: Practical Identity-Based Encyrption Without Random Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp.445-464. Springer, Heidelberg (2006)

[6] Ateniese G., Gasti P.: Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47. Springer, Heidelberg (2009)

[7] Ducas L.: Anonymity from Asymmetry: New Constructions for Anonymous HIBE. In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 148-164. Springer, Heidelberg (2010).