Secure Transmission of Information Using Key Management by Elliptic-Curve Cryptography

Ruby Singh
Assistant Professor, Dept of IT,
SRM University, NCR Campus
Modinagar
rubysinghit@gmail.com

Pramod Kumar Sagar
Assistant Professor, Dept of IT,
SRM University, NCR Campus
Modinagar
pramodsagar.srm@gmail.com

Kanika Garg
Assistant Professor, Dept of IT,
SRM University, NCR Campus
Modinagar
kanikagarg.kg@gmail.com

ABSTRACT

The basic concept of providing the data to the user should be based on the key management such as in electronic subscription and pay channel systems. In the proposed system, we are forming the key assignment scheme for access control information for efficiency and security. We are keeping the master key as a secret that data should be organized and then it should be broadcast to the users providing them with some privileges and the data are to be stored in the Tamper-Resistant Devices. It should be managed in efficient way by using Elliptical curve cryptographic key algorithms. An ideal time-bound key management scheme should be able to perform the task in an efficient fashion and minimize the storage and communication of keys. Elliptic-Curve Cryptography (ECC) is deployed in this scheme to overcome large computational load, high implementation cost and to enhance security & efficiency.

KEYWORDS— Tamper-Resistant Device, Elliptic-Curve Cryptography, time-bound key management.

1. INTRODUCTION

In a Web-based environment, the data to be securely broadcast, can be organized as a hierarchical tree and encrypted by distinct cryptographic keys according to access control policies. We need a key management scheme so that a higher class can retrieve data content that a lower class is authorized to access, but not vice versa. In many applications, there is a time bound associated with each access control policy so that a user is assigned to a certain class for a particular period of time. The problem of key management in hierarchical access control is important for many applications and has received significant attention in the research literature. All users are divided according to the policy configuration classes – so called security classes – and each access class has a set of resources associated with it. The classes arise when a class inherits the privileges of its subordinates, and thus a user at a specific class obtains access to the resources at his/her own class and all descendant classes in the hierarchy. The model is such that resources are kept encrypted under certain keys, and access to a decryption key implies access to the resources secured with that key.

For efficiency reasons, access is often based on key derivation: users receive one or a small number of keys that allow them to obtain access to the authorized objects without interacting with the server, through a key derivation process. It is clear that low requirements allow a scheme to be used in a much wider spectrum of devices and applications (e.g., inexpensive smartcards, small battery-operated sensors, embedded processors, etc.) than costly schemes. Thus, the objective of key management in hierarchical systems is to assign keys to users and resources such that access rights are efficiently and correctly enforced. Efficiency in key management schemes is usually measured by a number of criteria, which are (in order of significance):

• The number of secret keys (or the size of private information) each user must store.

• The amount of computation a user needs to perform to obtain access to the desired resource.

• The work needed to perform when the singleton policy configuration or set of users change and the degree to which users' private keys are affected.

• The size of information the system must maintain.

The tools that are used are:

- Tamper-Resistant Device
- Secure hash function
- Elliptic curve cryptography(ECC)

1.1 Tamper Resistant Devices

The tamper-resistant device plays an important role in our scheme. The system's master key K must be protected by the device. A leakage will not help the attackers much, because they are not able to compute the HMAC, thus the temporal class keys, without knowing K. Unless Master key is discovered, the attacks to retrieve on individual devices are not effective. With the use of a tamper-resistant device, the security of the scheme is strong enough. Attacks on tamper-resistant devices need special equipment. It is cheaper to buy a subscription than the special equipment. As such, the attacker does not have economic incentives to mount such an attack, unless he could capture the master key. An attacker who could find all the information on several tamper-resistant devices could execute a collision attack to compute extra temporal decryption keys. As pointed out above, the only information that needs to be kept secret by the tamper-resistant device is the system's master key.

2. PROBLEM DESCRIPTION

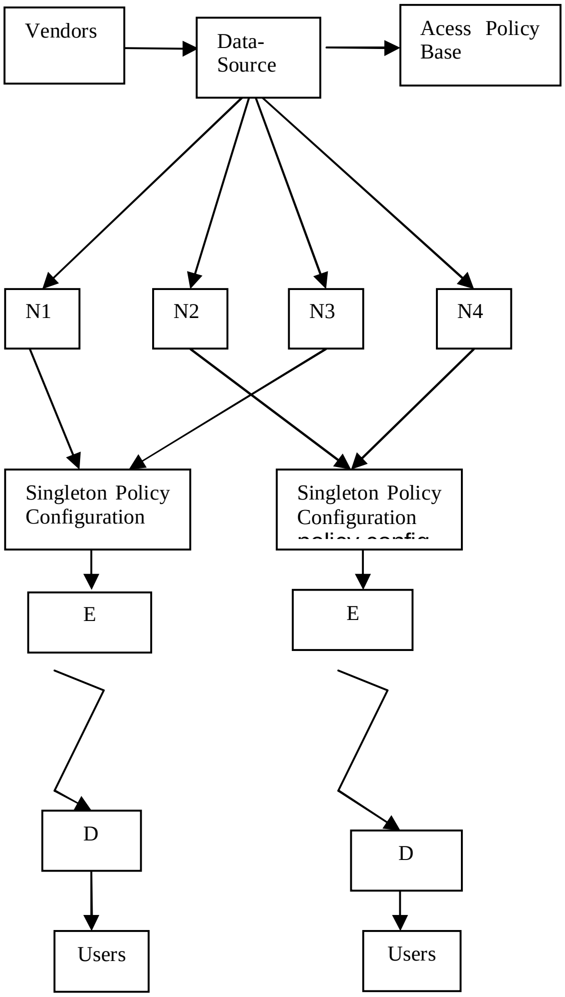
2.1 Issues in the previous work

- The number of all keys storing all needed decryption keys in a tamper-resistant device are causes excess computational storage.
- Excess computational storage causes the collision attack.
- If the system's class keys need to be updated, all devices containing these keys must be discarded, and new devices need to be issued.
- Tamper-resistant device and the hash functions have been proven not to be clashes free, but it is still hard to find a reimage to a given digest in a reasonable time.

3. PROPOSED WORK

- The new key assignment scheme for access control policy using elliptic- curve cryptography is more efficient and secure.
- This time bound hierarchical key management performs task to minimize the storage and communication of keys.
- The Tamper-resistant device the data can be access by the keeping master key as secret. So that it can be protected. The users can change the class keys of the system at anytime without having in different form of new devices to user.
- The device is tamper resistant in the sense that no one can recover the key change or change the time of the clock.
- The attacks on smart cards and some other tamper-resistant devices, such attacks require special equipment, which would cost more than a Subscription.
- The attackers are not able to perform the HMAC operations. Therefore, an attack relying on the knowledge of K is not feasible in practice. We believe that the use of the tamper-resistant hardware is practical and secure in reality.

4. OVERALL BLOCK DIAGRAM


Vendors
Data-Source
Acess Policy Base
N1
N2
N3
N4
Singleton Policy Configuration
Singleton Policy Configuration
E
E
D
D
Users
Users

N-Node

E-Encryption

D-Decryption

5. CONCLUSION

A large volume of work on key assignment schemes, this scheme gives the solution for the security and supports without the need for key re-distribution to the current users. Our system is also one of the most efficient and at the same time simple solutions to date. These techniques were also proven very useful in extending the key management solutions to time and access based in formations. An efficient time-bound hierarchical key management scheme based on the use of elliptic-curve cryptography (ECC) for secure broadcasting of data. The number of encryption keys to be managed depends only on the number of access control information. A tamper-resistant device plays an important role in our scheme. The obvious solution of storing all needed decryption keys in a tamper-resistant device is not practical, because the number of keys needed can be large. The time is also in particular period of intervals and access keys and privileges can also changes on time. In addition, with such a solution, when the system's class keys need to be updated, all devices containing these keys must be discarded, and new devices need to be issued.

REFERENCES

[1]. M. Atallah, M. Blanton, and K. Frikken, "Incorporating Temporal Capabilities in Existing Key Management Schemes," European Symposium on Research in Computer Security (ESORICS'07), Sep. 2007.

[2]. M. Atallah, M. Blanton, and K. Frikken, "Efficient Key Derivation for Access Hierarchies," CERIAS Technical Report TR 2007-30, Purdue University, Jun. 2007.

[3].A.De Santis, A. Ferrara, and B. Masucci., "Cryptographic key assignment scheme for any access control policy", Information Processing Letters (IPL), 2(4):19 205, November 2004.

[4]. W. Tzeng. "A time-bound cryptographic key assignment scheme for access control in a hierarchy",EEE Transactions on Knowledge and Data Engineering (TKDE), 14(1):182–188, 2002.