A NEW GROUP KEY MANAGEMENT STRUCTURE FOR FRAUDULENT INTERNET BANKING PAYMENTS DETECTION

Osama Dandash, YilingWang
Faculty of IT, Monash University, Australia

Phu Dung Le, Bala Srinivasan
Faculty of IT, Monash University, Australia

Keywords: Internet Banking Payments, Fraud Detection, Dynamic Individual Key and Group Key.

Abstract: Fraudulent payments detection in the banking system is an extremely important form of risk management as the industry loses close to one billion dollars annually. New techniques in detecting fraud are evolving and can be applied to many business fields. However; there is still no efficient detection mechanism able to identify fraudulent activity by employees. This paper presents a new Group Key Management (GKM) structure to facilitate internal fraudulent banking payments detection by dynamically combining an Individual Key (IK) and a Group Key (GK). The main objective of the proposed mechanism is to identify internal fraudulent users and trace their records amongst other group members.

1 INTRODUCTION

Internal fraud is the result of employees gaining access to customer information, creating false accounts and performing illegal transactions. Banks consider internal fraud as more damaging than external fraud (Zhuang and Fong, 2004).

Studies show that the internal fraud is defined as "acts by employees intended to defraud their financial institution by the misappropriation of funds and the authorisation of loans to unauthorized parties" (Patiwat P, 1996)(Zhuang Y, 2004). To identify fraudulent behaviour, advanced detection techniques are required and a high level authentication mechanism needs to be in place. This needs to not only identify fraudulent use but to also trace the activity. Better fraud detection has become an essential requirement for banks in order to maintain a viability payment system.

At present, fraud detection is conducted using data mining, statistics, and artificial intelligence (Ghosh, S, 1994)(Joris C, 2002)(Ren, D, 2004). Such methods still lack sufficiently secure payment mechanisms to identify internal fraud and trace fraudulent transactions.

Inadequate security operations, such as staff identification, staff access control and staff record tracing has resulted in insecure transaction (Jon M, 2003)(Medvinsky, G, 1993). To combat this security breach, this paper proposes a new Group Key Management GKM structure facilitates fraudulent payments detection by dynamically combining both an Individual Key IK and a Group Key GK. The objective of this proposal is to detect and trace fraudulent use by internal workers.

The proposed detection mechanism will record the details of each user separately even if two users from the same group access identical information. The role of GKM is to restrict user access to different objects in the system. GKM performs communication securely and efficiently and consists of a set of protocols that perform sensitive information transactions.

This paper is presented in the following sections: Section 2 relates to banking payments fraud detection methods. Section 3 presents the proposed GKM structure. Section 4 details the proposed structure's advantages. Section concludes our work.

Dandash O., Wang Y., Dung Le P. and Srinivasan B. (2007).
A NEW GROUP KEY MANAGEMENT STRUCTURE FOR FRAUDULENT INTERNET BANKING PAYMENTS DETECTION.
In *Proceedings of the Ninth International Conference on Enterprise Information Systems - SAIC*, pages 57-62
DOI: 10.5220/0002356800570062

2 RELATED WORK

The following subsections provide an overview of banking payments fraud detection methods to date.

2.1 Outlier Detection

An outlier relies on observation techniques to trigger suspicion that it has been generated by a different mechanism. It detects fraud in two ways: supervised and unsupervised.

Supervised detection relies on stored fraudulent transactions. This requires previous fraudulent use before any future fraud can be detected. Unsupervised detections does not rely on previous fraud cases but focuses on unusual transaction behaviour (Angiulli, F, 2006)(Ren, D, 2004).

2.2 CardWatch

This relies on the current patterns of use to detect possible anomalies. A Falcon skilled at many different types of propagation algorithms uses feed-forward Artificial Neural Networks is used to detect fraud (Ghosh, S, 1994).

Such training algorithms include machine learning, adaptive Pattern Recognition, neural networks, and statistical modelling. These are used to improve the way the developed Falcon can predict specific fraudulent transactions.

Neural MLP-based classifier is another detection method uses neural networks. It does not rely on previous fraud cases or historic data; instead it uses the information of the operation itself and of its instant previous history (Xiu Li, 2004).

Such technologies have the following disadvantages:

- They only rely on fraud attempts that have previously occurred to detect another fraud
- They are unable to identify who has performed the fraudulent transaction
- They rely on users sharing the same fixed secret information for a long period of time and applying weak cryptographic keys that could be attacked after a limited number of attempts
- They have weak fraud detection ability as they don't apply strong access rules.
- They are lack of a mechanism to specifically deal with security and trust issue, associated with internal user behaviour.

3 PROPOSED GROUP KEY MECHANISM

Identifying internal fraudulent use and tracing the activity is the most efficient way to deal with security issues. This also allows evidence to be harnessed to track down and prosecute the perpetrators of fraud. Many group key management approaches have been proposed and implemented in the wireless and multicast environment. GK is yet to be applied to Internet payments fraud. The most GK efficient approach is the Logical Key Hierarchy (LKH) (Harney H, 1997).

In LKH, a key tree is formed by GK and other auxiliary keys, which are used to distribute the GK to the users. Figure 1 depicts a typical LKH key tree where users are associated with the leaf nodes. Each user must store a set of keys along the path from leaf node up to the root.

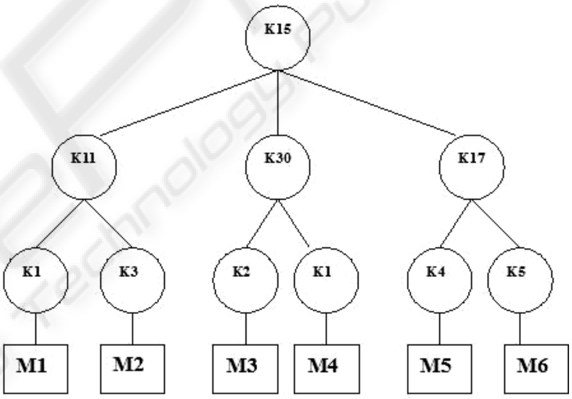

Figure 1: LKH Key Tree.

3.1 Notations

- A/R: Accept/Reject
- M: User
- Req/Res: Request and Response
- JReq: Join Request
- AccReq: Access Request
- AuthReq/AuthRes: Authentication Request and Authentication response
- Act: Activities
- AC: Account
- GC: Group Controller
- IK: Individual Key
- GK: Group Key
- S: System
- SP: Secret Phrase
- BC: Banking Card

- h(v): hashed value
- H: History
- T: Transaction
- LT: Log on Time

3.2 Proposed System Structure (User Authentication and Access Controls)

The banking system is divided into several administrative areas. Each administrative area consists of several branches and each branch applies a GKM structure which will provide data security and strong access control. The top level in the banking structure is called a Centralised Key Management (CKM). CKM is responsible for coordinating the groups' information in each branch, generating group keys and distributing them to the branches group members as shown in Figure 2.

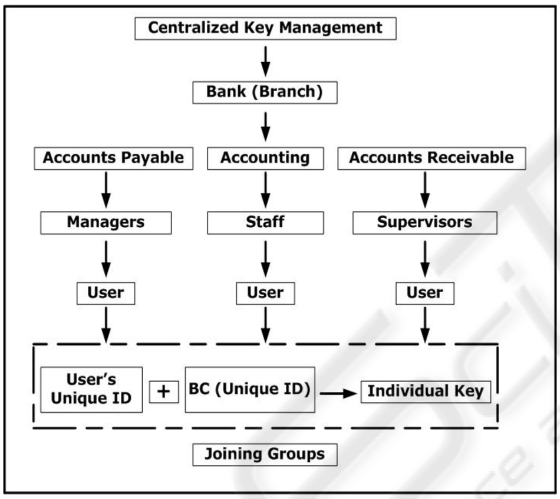

Figure 2: Proposed Group Key Management Structure.

Strong authentication, authorization and access control policies are enforced in each department to assign various roles to the groups and their members such as executives, directors and managers. Therefore, each group has different access privileges in which a strict access control can be achieved to allow only authorized members to access confidential information.

When changes in membership status take place (join leave), the re-keying procedure is invoked to update the keys along the path thereby ensuring security. In the banking system, the internal users are quite stable and can be grouped by the branch. Therefore they are physically and logically neighbours in LKH tree. This significantly reduces the communication cost during the re-keying procedure.

Based on this structure, each group member is assigned, or holds, an IK and a GK. To trace each payment transaction, the concept of dynamically combining IK and GK to generate a tracing hashed value *h*(v) is introduced into the structure.

3.2.1 User Registration

When users wish to join a group, they must register with the Group Controller GC by providing their personal information and biometric identification. Registered users will be issued a Secret Phrase (SP) and a Bank Card (BC) with a unique ID. This will be combined with users' unique ID to form an Individual Key (IK). If registered, the BC will hold users' IK for later authentication and authorisation purposes.

The joining procedure begins with a registration request sent by the user M to GC.

$$M \rightarrow GC: \{JReq\} \qquad (1)$$

Upon receiving, GC asks for personal information and user's unique ID:

$$GC \rightarrow M: \{M_{ID}, M_{PI}, Req\} \qquad (2)$$

Where

$$M_{ID} = \{\text{Finger Print, Retinal Scan, DNA, Face or Voice recognition, etc}\}$$

The user has to respond with the requirements to be legible for registration:

$$M \rightarrow GC: h\{M_{ID}, M_{PI}, Res\} \qquad (3)$$

Based on the provided details, GC generates a GK for the new member:

$$GC \rightarrow \{GK_M\} \qquad (4)$$

GK will be stored on GC side for later authorization while IK will be shared between GC and M.

3.2.2 System Accessibility (Dynamic Token Generation)

Registered users will need to have identified themselves to their BC at the start of each transaction by providing their registered unique ID.

$$M \rightarrow BC: h\{AuthReq, M_{ID}\} \qquad (5)$$

$$BC \rightarrow M: \{AuthRes, A/R\} \qquad (6)$$

If the provided M_{ID} is legitimate then authentication to the BC will be granted. The IK will generate a dynamic Token, which will be sent to GC to match with the other token that is generated on GC side:

$$BC \rightarrow GC: \{AccReq, Token\} \quad (7)$$

$$GC \rightarrow BC: \{AccRes, A/R\} \quad (8)$$

If Tokens match, then GC will send a GK for that registered M to grant access to S:

$$GC \rightarrow BC: \{GK\} \quad (9)$$

The sent GK will be combined with the generated Token on BC to generate a *h*(v):

$$BC \rightarrow S: h(v) \quad (10)$$

$$h(v) = \{GK, Token\} \quad (11)$$

The generated *h*(v) will be recreated each time an individual accesses S, which makes it secure and hardly guessable.

3.2.3 Record Tracing

An internal M could emulate the holder of a genuine client's account and accesses S to perform anonymous fraudulent transactions. To be able to detect such behaviour, it is proposed that *h*(v) be generated based on the users' unique ID and his/her GK. This means no authentication will be granted for any user to the BC if he/she cannot provide a genuine unique ID. No GK will be sent unless the generated Tokens are matched.

Moreover, the proposed mechanism in generating *h*(v) is more secure than the normal authentication log on process as it attaches to a log on sessions and allows the internal users to be traced and all their details recorded into the system each time they access it.

The recorded details will be the History (H) of those users, which can be reviewed and checked in the case of any suspicious activities or illegal transactions:

$$\text{Let } h(v_i) = \{GK_i, Token_i\} \quad (12)$$

Where i is the index of the *h*(v),

h(v) traces and records users' details. The recorded details or H will consist of the users' identity, their activities and the Transactions T they have performed:

$$H: = \{M_{ID}, AC, T\} \quad (13)$$

Where,

M = {BC_{ID}, GK, login-name, LT, password}
AC = {M_{ID}, account holder name, transaction ID, account balance, Date}
T = {Time-stamp, IP address, source transaction, destination transaction}

The dynamic combination mechanism ensures that every access to the system can be traced and will discourage fraud attempts. In case of any fraud reported, the system can easily identify the fraudulent users and the details of their fraudulent transactions.

From a technical point of view, once a transaction is detected as a fraud, then all the parameters can be used to detect and trace any other fraudulent transactions.

4 THE ADVANTAGES OF THE PROPOSED STRUCTURE

The GKM can assure access detection, record tracing, identify data integrity and ensure high-level authentication. In this section the advantages of the proposal are detailed.

- The proposal provides a strong authentication mechanism with dynamic IK generation. Although the current existing authentication systems use a combination of the user's personal details in addition to other technology such as smart cards in identifying users, the unique ID remains static (the same key is used every time). This weakness gives intruders enough time to reveal the secret and break into the system. In the GKM system the focus is on making the generation of the critical keys dynamic. This makes the key unbreakable. Intruders may decrypt the key in a very short time with the explosive increase of computation power but it is useless due to the constant change of key generation.

- The proposal uses GK to enforce access control restriction. It is applied to restrict the users to critical data, which provides extra secure protection to the access control. Due to the stable organization structure of the banking system, an optimized LKH algorithm is applied to manage the distribution of GK. This significantly reduces the communication cost during the re-keying. In traditional LKH, the communication cost of new users and redundant keys (joining and leaving) are $\log_\alpha n+1$ and $\log_\alpha n$, n is the number of users and α is the degree of the key tree. The cost in the proposal is as follows:

$$\log_\alpha\left(\frac{n}{i}\right)+1 \qquad (14)$$

and

$$\log_\alpha\left(\frac{n}{i}\right) \qquad (15)$$

Where, *i* is the number of branches.

- The proposal provides strong data integrity which shows that the messages were generated from the claimed users and are not modified in transmission by group members or external adversaries. This specification supports this requirement based on the strict authentication and through the use of a one-way hash function. Each generated hashed message has a unique value so that any change to the message will produce a different value and will cause the verification process to fail.
- The proposal provides user identification and record tracing.
  - The generated hashed value in conjunction with the combination of unique ID and GK can assure the identity of the originator of the message. Also, the use of a one-way hash function provides a high degree of certainty that the message was generated by M. A similar mechanism is used in the response messages that sent back to M from the GC, thus providing a high degree of certainty that the response is indeed from the GC. It is therefore a strong proof that messages were transmitted by M and GC
  - Each transmission performed by users will be recorded in the system by the generated h(v). The recorded parameters will provide a complete tracking mechanism to identify users and their activities. Therefore, users cannot deny the actions they performed in the system.

5 CONCLUSION

This paper proposes a new structure which can detect fraud by dynamically combining IK and GK. The new structure has the ability to identify users, manage them into groups, trace their activities and verify their authorization level. It also applies restricted access control and employs security policies which assign and manage different rules and privileges for users that may belong to same group.

REFERENCES

Angiulli, F.; Basta, S.; Pizzuti, C.; Feb. 2006: "Distance-based detection and prediction of outliers " Knowledge and Data Engineering, IEEE Transactions on Digital Object Identifier 10.1109/TKDE.2006.29 Volume 18, Issue 2, Feb. 2006 Page(s):145 – 160

Donal O'Mahony, Michael Peirce, and Hitesh Tewari. Electronic Payment Systems for E-Commerce. Artech House, 2001. Second edition.

Ghosh, S.; Reilly, D.L, "Credit card fraud detection with a neural-network", 1994, IEEE System Sciences,. Vol.III: Information Systems: Decision Support and Knowledge-Based Systems, Proceedings of the Twenty-Seventh Hawaii International Conference on , Volume: 3, pp.621-630, 4-7 Jan. 1994

Harney H., Andrea Colegrove and Patrick McDaniel. "Principles of Policy in Secure Groups" . Proceedings of Network and Distributed Systems Security 2001. Internet Society, February 2001. San Diego, CA

Harney H. and Muckenhirn C., 1997 "Group Key Management Protocol (GKMP) Architecture" RFC 2094,

Jan C, Jean-Marc Piveteau, and Markus Stadler. An Efficient Fair Payment System. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, pages 88{94, March 1996.

Jon M. Peha, Ildar M. Khamitov, "PayCash: 2003, a secure efficient Internet payment system", Proceedings of the 5th international conference on Electronic commerce, Pittsburgh, Pennsylvania, pp.125-130,

Joris C, Valentin Dem, Danny De Cock, Bart Preneel, and Joos Vandewalle. 2002, On the Security of Today's Online Electronic Banking Systems. Computers & Security, 21(3):253{265,

Medvinsky, G. & Neuman, B. C. (1993). Netcash: A design for practical electronic currency on the internet. Proceedings Of First ACM Conference On Computer and Communication Security, ACM.

Patiwat P, "Money in electronic commerce: digital cash, electronic fund transfer, and Ecash", 1996 Communications of the ACM, Volume 39, Issue 6, pp.45-50,

Ren, D.; Rahal, I.; Perrizo, W.; 2004 "A vertical outlier detection algorithm with clusters as by-product" Tools with Artificial Intelligence, 2004. ICTAI 2004. 16th IEEE International Conference on Digital Object Identifier 10.1109/ICTAI.2004.22, 15-17 Nov. 2004 Page(s):22 - 29

Rodeh O.,et al.,"Optimized Group Rekey for Group Communication Systems" Network and Distributed System Security 2000, San Diego, CA , February 2000

Sherman A.T., McGrew D.A., “Key Establishment in large dynamic Group Using One-Way function Trees” IEEE on software engineering vol. 29, no. 5, 2003, pp. 444-458

Thomas Hardjono, Mark Baugher, Hugh Harney, "Group Key Management for IP Multicast: Model & Architecture," wetice, p. 223, Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001.

Wong C., Gouda M., Lam S., 2000 “Secure Group Communications Using Key Graphs” IEEE networking vol. 8, no. 1, pp. 16-30

Xiu Li; Bing Li; Lin Lei; Jianyong Tuo; Shouju Ren; Wenhuang Liu; 2004 Artificial immune system for fraud detection Systems, Man and Cybernetics, 2004 IEEE, Volume 2, Page(s):1407 - 1411 vol.2,Digital Object Identifier 10.1109/ICSMC.2004.1399827

Zhuang Y, Simon Fong, 2004 On Designing a Flexible E-Payment System with Fraud Detection Capability, 2004 IEEE