RESEARCH ARTICLE OPEN ACCESS

AUTHENTICATION WITH ENHANCED PRIVACY USING FILE STREAM SEQUENCING TECHNIQUE

Manikandan.R[1], R.J.Poovaraghan[2]
[1]Research Scholar Department of CSE,
[2]Assistant Professor, Department of CSE,
SRM University, Ramapuram Campus,
Chennai-600089

----------**********----------

Abstract:

Authentication is the most common and essential Service of Information Security. User authentication protocol plays a vital role in payment schemes. The main concept of oPass is to free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, oPass involves a component which is used to generate one-time passwords and a communication channel, mail ids which is used to transmit authentication messages. In our opinion, it is difficult to thwart password reuse attacks from any scheme where the users have to remember something. We also state that the main cause of stealing password attacks is when users type passwords to untrusted public computers. In order to make the communication more secure, the user logins by providing the graphical password. This graphical password is stored in the database when the user registers his/her account. This graphical password is limited to a certain pixels. When the user logins, he/she has to provide the graphical password of the given pixels. If the graphical password provided matches with the password stored in database, then the user is recognized as an authorized user. Else the user's access will be denied since he is an authorized person. We propose RACE, a Report-based payment scheme for MWNs. The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less.

----------**********----------

1. INTRODUCTION

Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, users must recall the selected passwords. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. The possible Factors of authentication are: Something the user knows, Something the user has, Something the user is.

Fig 1.1 Factors of Authentication

However, password-based user Authentication has a major problem that

humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack. The above problems are caused by the negative influence of human factors. Therefore, it is important to take human factors into consideration when designing a user authentication protocol. Up to now, researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure. Since humans are more adept in remembering graphical passwords than text passwords, many graphical password schemes were designed to address human's password recall problem. Using password management tools is an alternative.

These tools automatically generate strong passwords for each website, which addresses password reuse and password recall problems. The advantage is that users only have to remember a master password to access the management tool. Despite the assistance of these two technologies—graphical password and password management tool—the user authentication system still suffers from some considerable drawbacks. Although graphical password is a great idea, it is not yet mature enough to be widely implemented in practice and is still vulnerable to several attacks. Password management tools work well; however, general users doubt its security and thus feel uncomfortable about using it. Furthermore, they have trouble using these tools due to the lack of security knowledge. Besides the password reuse attack, it is also important to consider the effects of password stealing attacks. Adversaries steal or compromise passwords and impersonate user's identities to launch malicious attacks, collect sensitive information, perform unauthorized payment actions, or leak financial secrets. Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. Three-factor authentication depends on what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric). To pass the authentication, the user must input a password and provide a pass code generated by the token (e.g., RSA SecureID), and scan her biometric features (e.g., fingerprint or pupil). Three-factor authentication is a comprehensive defense mechanism against password stealing attacks, but it requires comparative high cost. Thus, two-factor authentication is more attractive and practical than three-factor authentication. Although many banks support two-factor authentication, it still suffers from the negative influence of human factors, such as the password reuse attack. Users have to memorize another four-digit PIN code to work together with the token, for example RSA SecureID.

2. RACE

RACE, a Report-based pAyment sChemE for MWNs. The nodes submit lightweight payment reports (instead of receipts) to the AC to update their credit accounts, and temporarily store undeniable security tokens called Evidences. The reports contain the alleged charges and rewards of different sessions without security proofs, e.g., signatures. The AC verifies the payment by investigating the consistency of the reports, and clears the payment of the fair reports with almost no cryptographic operations or computational overhead. For cheating reports, the Evidences are requested to identify and evict the cheating nodes that submit incorrect reports, e.g., to steal credits or pay less. In other words, the Evidences are used to resolve disputes when the nodes

disagree about the payment. Instead of requesting the Evidences from all the nodes participating in the cheating reports, RACE can identify the cheating nodes with submitting and processing few Evidences.

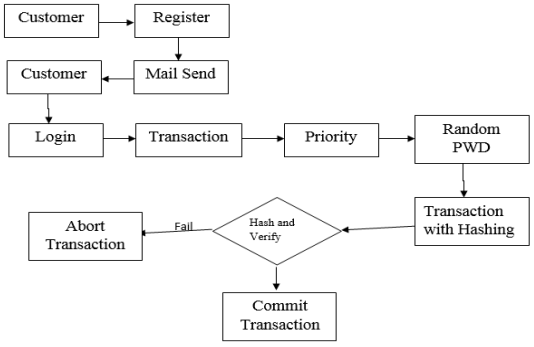
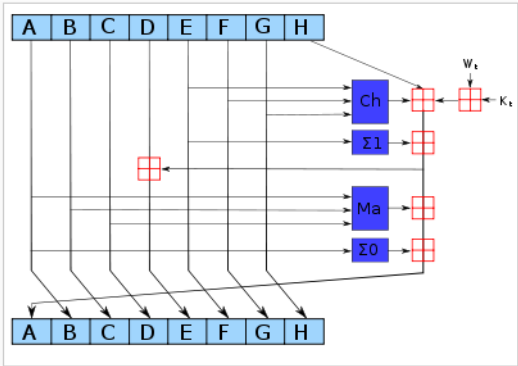


Fig 2.1 Flow Diagram of a RACE Transaction

Moreover, Evidence aggregation technique is used to reduce the storage area of the Evidences. In RACE, Evidences are submitted and the AC applies cryptographic operations to verify them only in case of cheating, but the nodes always submit security tokens, e.g., signatures, and the AC always applies cryptographic operations to verify the payment in the existing receipt based schemes. RACE can clear the payment nearly without applying cryptographic operations and with submitting lightweight reports when Evidences are not frequently requested. Widespread cheating actions are not expected in civilian applications because the common users do not have the technical knowledge to tamper with their devices. Moreover, cheating nodes are evicted once they commit one cheating action and it is neither easy nor cheap to change identities. Our analytical and simulation results demonstrate that RACE requires much less communication and processing overhead than the existing receipt-based schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary to make the practical implementation of the payment scheme effective. Moreover, RACE can secure the payment and precisely identify the cheating nodes without false accusations or stealing credits. Thus we add more security to our proposed system.

3. SHA-2 ALGORITHM

SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits.



One iteration in a SHA-2 family compression function. The blue components perform the following operations:

$$\mathrm{Ch}(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$\mathrm{Ma}(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The red ⊞ is addition modulo 2^{32}.

Fig 3.1 Compression Function of SHA-2 (One Iteration)

SHA-256 and SHA-512 are novel hash functions computed with 32 and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512. The cryptographic hash function SHA-256

(secure hash algorithm, FIPS 182-2) has a digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.

4. COLLECTED RESULTS

4.1 PERFORMANCE EVALUATION

Public-key cryptography is widely used to secure the wireless networks Using public-key cryptography in RACE is necessary to secure the payment because it enables the nodes to compose valid Evidences and enables the TP to identify the cheating nodes. Public-key cryptography technology and hardware implementation have been improved, and the signing and verifying operations can be performed by mobile nodes with acceptable overhead. In digital signatures can be computed efficiently in two steps. The offline step is independent of the message and performed before the message to be signed is available; and a lightweight online step is performed once the message to be signed becomes available. In FPGA implementation of the RSA cryptosystem can efficiently perform the signing and verifying operations in sever a millisecond. Moreover, the proposed communication proto cool in that transfers messages from the source to the destination nodes with limited number of public-key cryptography operations can be integrated with RACE, but the focus of this paper is on reducing the communication and the payment processing overhead.

4.2 STIMULATION SETUP

We run a simulator to evaluate the overhead of RACE. 50 mobile nodes with 150 m transmission range are deployed in a square cell of 1200 m by 1200 m. Constant-bit-rate traffic source is implemented in each node as an application layer and the source and destination pairs are randomly chosen. We use the modified random waypoint model to emulate the nodes' mobility. Specifically, a node travels towards a random destination that is uniformly selected within the network field; upon reaching the destination, it pauses for some time; and the process repeats itself afterwards. The nodes' speed is uniformly distributed in the range [0, S max] m/s, where S max is 5 and 10 m/s, and the pause time is 20 s. The data packets are transmitted with the rate of 0.5 packet per sec. We simulate the Dynamic Source Routing protocol (DSR) The time stamp (Ts), node's identity (IDi), and message number (X) are five, four, and two bytes, respectively, and the hash chain size is 35. The simulation results are averaged over 200 runs and presented with 95 percent confidence interval. Table 6 summarizes the simulation parameters. In the simulation, we consider 1024-bit RSA digital signature scheme because the verifying operations performed by the intermediate and destination nodes require less time than the signing operations performed by the source node. According to NIST guidelines, the secure private keys should have at least 1024 bits. For the hash function, we use SHA-1 with digest size of 20 bytes. We evaluate the expected processing delay due to performing the cryptographic operations by the mobile nodes using Crypto++5 library and a laptop with an Intel processor at 1.2 GHZ and 1 GB RAM. The computation times of signing and verifying operations are 15.63 ms and 0.53 ms, respectively, and the computation time of hashing a 512-byte message is 29 µs. The resource of a real mobile node may be less than a laptop so the measured computation times are scaled by the factor of five and considered as delays to simulate performing the cryptographic operations in a limited-resource node. From, the consumed energy for signing and verifying operations are 546.5 mJ and 15.97 mJ respectively, and the consumed energy for hashing a 512-byte message is 389.12 µJ.

4.3 STORGE OVERHEAD

The sizes of receipts, payment reports, and Evidences depend on the number of intermediate nodes because the nodes' identities are attached to them. Thus, changing the network parameters such as the network size, the nodes' radio transmission range and density, etc. will change the route length and have the same effect on RACE and receipt-based schemes. Table 7 gives the average size of receipt, report, and Evidence for RACE and receipt-based payment schemes. The receipt size of ESIP is larger than that of PIS due to attaching two hash values from the source node's hash chain and another two hash values from the destination node's hash chain. For Sprite, ESIP, PIS, and RACE, 1MB storage area can store up to 3531, 7282, 16425, and 10082 receipts and Evidences, respectively. Although PIS requires low storage area, it needs two signatures per message, i.e., one from the source node and another from the destination node. Several measures have been taken to reduce the Evidences' size in RACE. One Evidence is composed per session regardless of the number of messages instead of generating an Evidence per message. The node's signatures are hashed to reduce the PROOF size and different Evidences can be aggregated to a smaller-size compact Evidence. Moreover, the nodes of MWN are typically equipped with limited energy supplies and the network is characterized with limited bandwidth, and it is feasible to build cost-effective nodes with more than a gigabyte of Flash memory Therefore, storage area may not be the main concern, but bandwidth and energy are more scarce, i.e., reducing the amount of submitted data is more important than the size of stored data. As we will discuss in Subsection the amount of submitted reports in RACE is much less than that of receipt-based payment schemes.

4.4 COMMUNICATION OVERHEAD

The communication overhead depends on the number and the size of receipts and reports. The number of receipts a report generates in a session depends on the frequency of breaking the route between the source and destination nodes because a new receipt/report is generated when the route is broken, and therefore, the MAC layer and the simulation parameters will have the same effect on RACE and the receipt based payment schemes. From Table 7, RACE requires submitting only 23.84 bytes for each payment report. This amount of data is much less than those of the existing receipt-based payment schemes because security tokens, e.g., signatures, are always submitted in receipt-based schemes but they are submitted only in case of cheating in RACE. Even if there are many cheaters in the network, RACE requires less communication overhead than the existing receipt-based schemes because the cheaters are excluded once they commit a cheating action. A 512 KB data transmission is sufficient for submitting 1765, 3641, and 8192 receipts in Sprite, ESIP, and PIS, respectively, and submitting 21,992 reports in RACE. Table 8 gives the average amount of data to submit receipts and reports for ten-minute data transmission. The source and destination nodes are randomly selected and a new route is established each time the route between the source and destination nodes is broken. It can be seen that a large amount of data is submitted in Sprite because a receipt is generated per message and the receipt size is large. PIS requires submitting less amount of data than ESIP because its receipts' size is less as indicated in Table 7, but PIS requires two signatures for transmitting a message. The amount of data to submit reports in RACE is much less than those of the receipt-based schemes. Table 8 indicates that more reports and receipts are submitted at high node mobility because the routes are more frequently broken, i.e., the source node's messages are transmitted over a larger number of routes.

4.4 PAYMENT PROCESSING OVERHEAD

Tables 9 and 10 give the processing overhead for clearing the payment of ten-

minute data transmission at different node speed in terms of the number of cryptographic operations, the total energy cost, and the processing time, assuming that the TP is a laptop with an Intel processor at 1.2 GHZ and 1 GB RAM. The tables indicate that RACE does not need any cryptographic operations for clearing the payment in case of fair reports. The tables also give the overhead of verifying an Evidence with X messages. The simulation results indicate that the payment clearance overhead of RACE is much less than the existing receipt-based payment schemes. It can also be seen that more overhead is required at high node mobility because more receipts are generated due to breaking the routes more frequently, which shows that receipt-based payment schemes may not be efficiently applicable in case of high node mobility, but the nodes' speed has no effect on the payment clearance overhead in RACE if the reports are fair. The low payment processing overhead can reduce the complexity and provide flexibility to the practical implementation of the TP. Moreover, since the payment schemes use micropayment, the overhead cost should be much less than the payment for the effective implementation of these schemes. The communication and processing overhead of the receipts will be very large with taking into account the following facts: (1) the simulation results given in Tables 8, 9, and 10 are only for ten minutes data transmission; (2) the nodes contact the TP every few days because this connection may not be available on a regular basis and to reduce the communication overhead; and (3) once a route is broken, a new route is established with a new receipt, and thus multiple receipts may be generated per Session. For military and disaster recovery applications of MWNs, the network can be considered ephemeral because it is used for a specific purpose and short duration. In this paper, we adopt the network model used in that targets the civilian applications of MWNs where the network has long life and the nodes have long-term relations with the network. As illustrated in Fig. 1, the considered MWN has an offline trusted party (TP) and mobile nodes. The TP contains the accounting center (AC) and the certificate authority (CA). The AC maintains the nodes' credit accounts and the CA renews and revokes the nodes' certificates. Each node A has to register with the trusted party to receive a symmetric key KA, private/public key pair, and certificate. The symmetric key is used to submit the payment reports and the private/public keys are required to act as source or destination node. We assume that the clocks of the nodes are synchronized. The details of this synchronization process are out of the scope of the paper, but several mechanisms have been proposed to synchronize the nodes. Once the AC receives the payment reports of a session and verifies them, it clears the payment if the reports are fair; else, it requests the Evidences to identify the cheating nodes. The CA evicts the cheating nodes by denying renewing their certificates.

5. CONCLUSION

In this paper, we have proposed a report-based payment scheme for MWNs. The nodes submit lightweight payment reports containing the alleged charges and rewards (without proofs) and temporarily store undeniable security tokens called Evidences. The fair reports can be cleared with almost no cryptographic operations or processing overhead, and Evidences are submitted and processed only in case of cheating reports in order to identify the cheating nodes. Our analytical and simulation results demonstrate that our scheme can significantly reduce the communication and processing overhead comparing to the existing receipt-based payment schemes with acceptable payment clearance delay and Evidences' storage area, which is necessary for the effective implementation of the scheme. Moreover, RACE can secure the payment and

precisely identify the cheating nodes without false accusations.

In RACE, the AC can process the payment reports to know the number of relayed messages and the number of dropped messages by each node. In our future work, we will develop a trust system based on processing the payment reports to assign and maintain a trust value for each node in the network. The nodes that relay messages more successfully will have higher trust values, such as the low-mobility and the large- hardware sources nodes. Based on these trust values, we will propose a trust-based routing protocol to route messages through the highly trusted nodes (which performed packet relay more successfully in the past) to minimize the probability of dropping the messages, and thus improve the network performance in terms of throughput and packet delivery ratio. However, the trust system should be secure against singular and collusive attacks, and the routing protocol should make smart decisions regarding node selection with low overhead.

REFERENCES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications Over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] H. Gharavi, "Multichannel Mobile Ad Hoc Links for Multimedia Communications," Proc. IEEE, vol. 96, no. 1, pp. 77-96, Jan. 2008.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom '00, pp. 255-265, Aug. 2000.

[5] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey," Wiley's J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332, 2006.

[6] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[7] S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55, ACM.

[8] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.

[9] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in WWW '05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479, ACM.

[10] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," Financial Cryptography Data Security, pp. 1–19, 2006.

[11] R. Dhamija, J. D. Tygar, andM. Hearst, "Why phishing works," in CHI '06: Proc. SIGCHI Conf. Human Factors Computing Systems, New York, 2006, pp. 581–590, ACM.

[12] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[13] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, pp. 770–772, Nov. 1981.