Proceedings of National Conference on Recent Advances in Computer Science & Engineering (NCRACSE-2017)

International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 01, February 2017
ISSN: 2455-3778
http://www.ijmtst.com

Time-Bound Anonymous Authentication for Roaming Networks

K. Aruna Kumari[1] | T.Lavanya[2] | P.Ashok Chakravarthi[3]

[1,2,3]Chalapathi Institute of Engineering and Technology, Guntur, Andhra Pradesh, India.

To Cite this Article
K. Aruna Kumari, T.Lavanya and P.Ashok Chakravarthi, "Time-Bound Anonymous Authentication for Roaming Networks", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 01, 2017, pp. 98-103.

ABSTRACT

We propose an anonymous authentication protocol that supports time-bound credentials for efficient revocation. It is especially suitable for large scale network in roaming scenario. With our newly designed group signature scheme as a building block, a timestamp can be embedded to user secret key. No expired key can be used to authenticate, and hence naturally revoked users (e.g., due to contract expiration) are not required to be put into the revocation list. This makes our protocol much faster than previous roaming protocols in terms of revocation checking, which is a main part in verification.

KEYWORDS: *accountable privacy, anonymous roaming, applied cryptography, authentication, privacy, revocation.*

I. Introduction

In mobile communications, roaming means a device going from its home location to a different location where it will connect to a foreign network for services. It allows mobile users to have connectivity careless of their geographical location. Users can make or receive phone call and SMS, or even access to the Internet from their mobile devices in any place on the Earth, provided that it is under a registered network coverage. Prior to connecting to a new foreign network, authentication must be made to protect the user and the network service provider. Figure 1 depicts the authentication model.

Data confidentiality and authenticity are usually needed to protect communications between users and the foreign server. However, a full personal authentication may not be desirable especially when privacy is a concern. In the roaming scenario, it is desirable to keep mobile users anonymous from auditor as well as the foreign server unless the identity information becomes critical. It is often sufficient to verify whether a user is among a group of subscribers.

User cancellation is of great importance to roaming protocols. Due to various reasons (e.g., the subscription period of a user has expired), the foreign server needs to find out whether a roaming user is reverse. Any reverse user should not be allowed to enter the foreign network. Achieving practical and efficient user cancellation is one of the most challenging problems as it is naturally difficult to "take back" an electronic contention from users. It is especially important for any large scale network. For example, in China there are more than 1.2 billion mobile users[1] shared over 3 different operators. If there are only 0:1% users reverse each year, there are already 1 million users to revoke. A fast revocation mechanism should be designed for dealing with this big list. Many studies with focus on anonymity issue in mobile communications and verifications have been done in the past decade Some are specifically designed for roaming protocols. cancellation is not considered until some of the recent works [31], [20]. Similar to many existing anonymous verification primitives which support revocation, either all unrevoked users need to update their license regularly, or the server needs to perform extra steps in verification to check each member against a reverse list. As time goes by, the list will just become larger since the validation is unsigned. All kind of users to be reverse, including those who were authorized for a limited time period, will be added to the revocation list Eventually, it will include many such short-term members after their membership expiration. This will cause a serious bottleneck, as the foreign server has to check the whole revocation list for every single validation process, which often involves a cryptographic mechanism to ensure the privacy of the users.

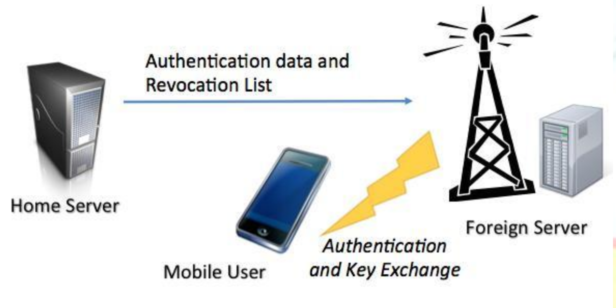

Fig:1 Authentication of Roaming Networks

At the first glance, N will certainly increase as more users are revoked. This explains why most schemes take the first approach to design more efficient revocation check, and the second draws little attention from researchers. One approach to “reduce” N is to make the system operates in epochs. However, this could boost up the size of the system parameter to be linear in the number of epochs. To have a closer look, verification phase in the authentication process consists of two steps: (1) “Validity Check” verifies if the authentication token is produced by a valid user; and (2) “Revocation Check” verifies if the user has been revoked. Existing approaches often make a decision regarding the validity checking based on a single dimension, without considering time-sensitive checking, i.e., a token’s validity may depend on the current time. Generally speaking, revocation can either be “natural” or “premature”. A user is “naturally revoked” when his access rights has expired, or a user can be prematurely revoked before the expiry time, say due to the compromise of the credential. We believe natural revocation accounts for most user revocation in practice and prematurely revoked users are only a small fraction. A better approach is to deal with natural revocation” in the stage for validity check instead. This paper investigates an efficient approach for such validitycheck.

A. Our Contribution

As argued, there are unique requirements for anonymous authentication in roaming, and the investigation of an efficient approach in this setting is of interest to both academia and industry. We propose an anonymous authentication roaming protocol, with the following distinctive features:

1. Each user secret key issued by the home server is bounded to an expiry time. It is infeasible to use an expired user secret key for successful authentication.
2. Our design leads to a shorter revocation list which only contains the information on prematurely revoked identities but not those expired naturally.
3. The overall computation time and cost in the authenti-cation will be greatly reduced since most of the portion are consumed by revocation check in situations where expired keys contribute most to user revocation.

Our scheme requires additional computation overhead in the verification, due to the checking of the expiry information embedded in the secret key. However, the additional cost is a constant and independent of the number of revoked users. Furthermore, when there are large number of users revoked due to expiration, the efficiency savings in our design, i.e., short revocation messages and fast revocation check, will far outweigh the efficiency loss incurred by the overhead. Our estimated performance shows that our protocol is several times faster (in the server side) than previous protocols that support revocation while the overhead induced in the user side is just a few seconds. We argue that in some large scale networks (e.g. mobile network in China that contains billion users), our protocol can be hundred times faster than previous protocols.

B. Enhancement over Our Conference Version

Compared with the conference version [17] which merely provides a cryptographic treatment of verifier-local revocation group signatures with time-bound keys, we not only identify a few distinctive requirements of authentication in roaming protocol and how this notion can be helpful, but also significantly extend the primitive into practical roaming protocol and further improve its efficiency via a new design. Directly using our old scheme [17] for authentication in our roaming protocol results in a communication transcript of size O(`), where ` is the bit-length for representing a time period. Here we further propose a new design with O(1)-size transcript by using the accumulator system [29], and simplify the encoding method of time period. Intuitions of the design behind our cryptographic construction will be given shortly.

II. Overview

A. Intuition

In our protocol, we require a group signature scheme as a primitive for both anonymous authentication and premature revocation. Group signature, introduced by Chaum and van Heyst [12], allows a member of a group to sign messages on behalf of the group without leaking his identity. But there is a group manager who has some trapdoor information which allows him to recover the identity of the signer from any valid group signature. A normal group signature cannot achieve our goal since the signature itself does not bear with any time-related information. Traditional revocation approach is inefficient since it either checks every entry in the revocation list or requires the manager to open all signatures.

Our main contribution is an efficient technique in realizing time-bound key which is integrable with our underlying newly designed group signature scheme. In the authentication phase, the foreign server gives a user U_i a challenge message m and a current time t. If U_i can generate a valid signature on m and prove that t <$_i$ where $_i$ is the key expiry time for user U_i, the foreign server believes that U_i is authorized by his home server and his secret key has not expired.

The data owner embeds the key expiry time in each secret key and the signature verification is done with respect to the current time. The time are encoded by the 0/1 encoding which reduces the “greater than” predicate to the “set intersection” predicate. So we do not need any range proof system which could be complicated. If there exists a common element between the sets of the two encoded time, which is done by simply checking the possession of one signature in a set of signatures for a range of [1; 2`], the verifier is convinced that the key expiry time is larger than the signing time. There must be an index k satisfying t_k = $_{ik}$. However, the user may not wish to leak this index information to the server because it may be used to infer the user’s identity. Our scheme allows the user to hide the index k in the authentication via the use of accumulator.

In our actual scheme, we introduce dummy strings to either $_{ij}$ when the corresponding set 1-ENC($_i$) (or 0-ENC(t)) has no length j element and each of these are all set to a special value denoted by “null”. All related steps in our proposed system involving “null” will be skipped. So, even when two sets both contain this special value, our scheme would not consider these sets to be having a common element just because of the existence of “null”.

B. Security Requirements

1) We require an anonymous authentication protocol for roam-ing networks to satisfy the properties below [31], [20]. Subscription Validation: the foreign server is sure about the identity of the home server of the user;
2) User Anonymity: besides the user and the home server no one including the foreign server can tell the identity of the user;
3) User Intractability besides the user and the home server, no one including the foreign server is able to identify any previous protocol runs which have the same user involved.
4) Provision of User Revocation Mechanism [31], [20]: due to various reasons (e.g., the subscription period
5) of a user has expired), the foreign server should be able to find out whether a roaming user is revoked;
6) Server Authentication: the user is sure about the identity of the foreign server;
7) Key Establishment: the user and the foreign server establish a random session key which is known only to them and is derived from contributions of both of them such that the home server cannot predict the value of it.

III. Proposed System

We first describe the new group signature scheme, which is followed by the complete description of our roaming protocol.

A. Our Newly Designed Primitive

We design a group signature scheme which allows users to authenticate themselves with both constant-size transcripts and full anonymity. It was unknown [17] how to achieve both simultaneously. The old approach [17] is that either full anonymity is achieved at the cost of transcript size logarithmic in the total number of supported time periods, or constant-size communication with weakened anonymity guarantee.

A group signature scheme consists of a tuple of probabilis-tic polynomial-time algorithms. During the group manager gen-erates a master public key gpk and a master secret key msk. gpk is published while msk is kept secret. During Gp.Join, the group manager uses msk to generate a user secret key gsk_i for user U_i and a revocation token grt_i which is used to trace user U_i. During Gp.Sign, a user U_i uses his secret key gsk_i to generate a signature for a message m at time t. Gp.Ver takes mpk; t; m; and returns valid or invalid

2) Exculpability: A group signature scheme is exculpable if no polynomial-time adversary can forge a signature that is attributed to an honest member such that the member cannot dispute. Here we assume the group manager is honest. Consider the game between an adversary A and a challenger C as follows.

Setup. C performs the initialization phase and obtains the result (gpk; msk). It sends A mpk. C prepares an empty revocation list RL.

Query. A issues the following queries to C.

Join: A requests for creating a new group mem-ber with a designated key expiry time. C per-forms the user joining phase locally and gets gsk_i for a new index i. A gets grt_i.

Corrupt(i): C returns the secret key gsk_i of user i to A and adds i to RL.

Sign(i; t; m): C returns the signature signed by gsk_i at time t, on message m or '?'.

Revoke(i): C returns the revocation token grt_i of user i and adds i to RL.

Forge. A outputs a message m, a signature and a revocation token grt, which must be one of those introduced in the Join process.

We say that A wins the game if

1) is a valid signature on m with the revocation list RL.

2) is not obtained from the signing queries with expiry time t on m .

3) is traced to a user with the revocation token grt.

3). Efficiency Analysis

We compare the performance of our scheme with two existing roaming protocols that support user revocation by Yang [31] et al. and He [20] et al. We first consider authentication at the user side. Public key operations are counted as follows: for signature scheme we deploy ECDSA [1] which takes 1 G_1 exponentiation operation for signing, and 1 for verification. We analyze the efficiency from an estimation based on the benchmark from jPBC [5] on the timing of various mathematical operations required in the system implementation. We count the number of basic operations required in various protocol and provide an estimation based on the benchmark of the jPBC library for the following devices:

Our estimation assumes that there are 1,000,000 users being revoked per year, including those naturally revoked (contract expired) and prematurely revoked (e.g. key compromised, phone stolen). We argue that this figure is reasonable in some large scale networks. For example, as of September 2013, there are more than 1.2 billion mobile users in China[6]. However, there are only 3 operators in the whole country. Each operator contains hundreds of million subscribers.

For our scheme, we divide into four different cases for consideration, according to the ratio

$$\frac{\text{naturally revoked users}}{\text{overall revoked users}}$$

with values 20%, 40%, 60%, and 80%. For the other two protocols, there is no difference regardless of this ratio.

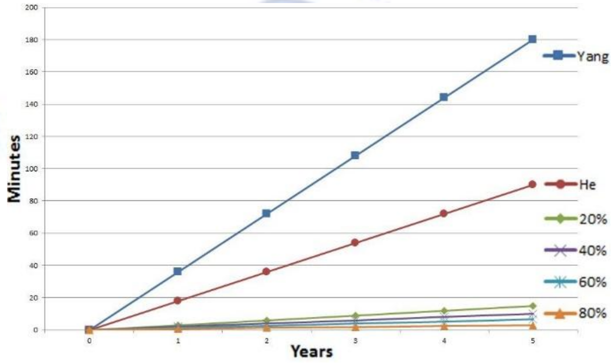

Fig. 3: Time to Check whether a user is in the Revocation List

To check whether a user is in the revocation list, it is required to check against all users in the list. The time thusgrows linearly. In Figure 3, we plot the time consumed for each user revocation checking (the time required to check whether a user is in the revocation list) as the Y-axis (0-200), against the number of years the system has been used as the X-axis (0-5). Again, we use some existing results from jPBC.

It is worth noting that the server in reality may be more powerful and support parallel processing, e.g., a octacore processor, and the running time can be shortened significantly. Another way is to divide the revocation list into n pieces and give it to n computers for checking independently. However, the ratios of running time between our scheme and other schemes remain the same. Moreover, we believe in most of the cases, the majority in the revocation list (say, at least 60%) are naturally revoked. From Figure 3 we can see that if the server uses a 2.4 GHz processor, our scheme takes about 6 minutes (after the system has been running for 5 years) if 60% of the list are naturally revoked users. Yang's scheme takes 180 minutes while He's scheme takes 90 minutes. Even if there are 10 computers for parallel processing, Yang's scheme still takes 18 minutes while He's scheme takes 9 minutes. Our scheme only requires 0.6 minute and 0.3 minute for 60% and 80% users who are naturally revoked, respectively. From the result, we can see that although our protocol requires more computation on the user side during the authentication process (about 4 seconds in our simulation), the time is still acceptable even for a 1GHz processor device (the overall running time is still around 6 seconds). On the other hand, the roaming server requires much less computation time for the revocation checking. The time should be practical enough to be deployed in real life scenarios. By having an efficient revocation checking, our protocol actually improves the performance of the whole roaming authentication protocol.

IV. CONCLUSION

We proposed an anonymous authentication roaming protocol that supports efficient revocation of naturally expired credentials. It relies on the underlying newly designed group signature scheme which can bind the expiry time to the secret key of every user. With this new feature, expired keys are no longer needed to be included in the revocation list since the authentication token generated by those keys will be invalid. This results in a significant efficiency improvement for revocation checking, due to the elimination of the expired keys in the revocation list. Moreover, compared with the conference version of this paper, we described the complete roaming protocol instead of just the group signature primitive. We further reduced the underlying group signature size from O(`) to a constant size, where ` is the bit-length for representing a time period, without losing any user anonymity. This makes our construction more practical in the roaming network environment.

REFERENCES

[1] ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1999. Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-Trapdoor Anonymous Tags for Traceable Signatures. Int. J. Inf. Sec., 12(1):19–31, 2013.

[2] Tolga Acar, Sherman S. M. Chow, and Lan Nguyen. Accumulators and U-Prove Revocation. In Financial Cryptography and Data Security, pages 189–196, 2013.

[3] Man Ho Au, Apu Kapadia, and Willy Susilo. BLACR: TTP-Free Blacklistable Anonymous Credentials with Reputation. In NDSS, 2012.

[4] Man Ho Au, Joseph K. Liu, Willy Susilo, and Tsz Hon Yuen. Secure ID-based Linkable and Revocable-iff-Linked Ring Signature with Constant-size Construction. Theor. Comput. Sci., 469:1–14, 2013.

[5] Man Ho Au, Willy Susilo, Yi Mu, and Sherman S. M. Chow. Constant-Size Dynamic k-Times Anonymous Authentication. IEEE Systems Journal, 7(2):249–261, 2013. Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In EuroCrypt, volume 2656 of LNCS, pages 614–629. Springer, 2003.

[6] Dan Boneh and Xavier Boyen. Short Signatures Without Random Oracles. In EuroCrypt, volume 3027 of LNCS, pages 56–73. Springer, 2004.

[7] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. In CCS, pages 168–177. ACM, 2004.

[8] Ernie Brickell and Jiangtao Li. Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. IEEE Trans. Dependable Sec. Computer, 9(3):345–360, 2012.

[9] Julien Bringer and Alain Patey. VLR Group Signatures - How to Achieve Both Backward.

[10] Joseph K. Liu, Cheng-Kang Chu, Sherman S. M. Chow, Member, IEEE,Xinyi Huang, Man Ho Au, Member, IEEE, and Jianying Zhou, 2014.2366300.