Privacy-Preserving Universal Authentication Protocol using Hierarchical Key and Group Signature

S. Ravikumar[1], A. Marimuthu[2], Ph.D
[1]MPhil Scholar, Government Arts College, Coimbatore

[2]Associate Professor, Government Arts College, Coimbatore

ABSTRACT
A novel protocol to achieve privacy-preserving universal authentication protocol for wireless communications called Priauth. Verifier-Local Revocation Group Signature with Backward Unlinkability (VLR-GS-BU), it can satisfy all requirements.Priauth belongs to the class of Universal Authentication Protocols in which same protocol and signaling flows are used regardless of the domain (home or foreign) a roaming user is visiting. Allowing people to get connected seamlessly using their devices without being limited by the geographical coverage of their own home networks roaming service should be deployed. The key is used to encrypt data transmitted to the servers or users. The efficient distribution of the new key for multiple membership changes is a critical problem in secure group communication. The goal of the enhancement is to evaluate trade-off between storage and revocation cost. Storage is computed in terms of keys that each user (respectively, VA) maintains and revocation cost is computed in terms of the encryptions performed, and the number of messages transmitted by the VA.

Keywords
Priauth, Hierarchical Key Management, Rekeying, Storage Trade-Offs.

1. INTRODUCTION
Wireless communications technologies have undergone rapid development. Small mobile devices within range of a wireless network can transfer data at any place and any time. This is bringing forth the important issue of information security, privacy, and authentication in an open space. Privacy involves ensuring that an eavesdropper cannot intercept the communication information of mobile users. Authentication involves ensuring that the services are not obtained fraudulently.

A privacy-preserving user authentication scheme should satisfy the following requirements:

(1) 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. In particular, the home server should not know the session key.

(2) User anonymity: besides the user and its home server, no one including the foreign server can tell the identity of the user; and

(3) User untraceablility: besides the user and its home server, no one including the foreign server is able to link any past or future protocol runs of the same user.

By introducing Verifier-Local Revocation Group Signature with Backward Unlinkability (VLR-GS-BU), it can satisfy all requirements described above. Priauth belongs to the class of Universal Authentication Protocols [2] in which same protocol and signalling flows are used regardless of the domain (home or foreign) a roami-ng user is visiting. This helps reducing the system complexity in practice. The VLRGS-BU is not originally designed for authentication purpose and a direct application of it imposes two problems in Priauth. Firstly, it does not allow Priauth to support new group member joining after system setup. Secondly, it does not provide Priauth the single registration property commonly available in most existing authentication protocols, which requires a user only to register once at the home network before being able to access the global network. We will provide solutions to these two problems to make Priauth practical.

2. RELATED WORKS
G. Yang, Q. Huang, D. S. Wong[2] propose a novel set of solutions to achieve secure roaming. Their solutions only require the roaming user □ and the foreign server □ to be involved in each protocol execution, and □ can be off-line. Furthermore, this protocol is identical to the authenticated key exchange protocol performed between □ and □ when □ is in its home network. All the existing three party protocols require a serving network to separate foreign users from local ones and perform different signaling flows respectively. They call such kind of authentication protocols Universal Authentication Protocols. In their solution, they achieve this objective efficiently and at the same time, maintain high scalability with respect to large numbers of revoked users.

M. Zhang and Y. Fang[6] they proposed that the protocol 3GPP AKA is vulnerable to a variant of false base station attack. The flaw of 3GPP AKA allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use the authentication vectors corrupted from one network to impersonate other networks hence the corruption of one network may jeopardize the entire system. The redirection attack represents a real threat since the security levels provided by different networks are not always the same.

3. PROPOSED SCHEME
In the proposed approach we have enhanced that in this protocol VA needs to interrupt the communication during the rekeying; the resulting delay can be unreasonable for many applications. One approach to revoke multiple users is to associate a key with every nonempty subset of users in the group. Thus, if one or more users are revoked, the VA uses the key associated with the subset of the remaining users to encrypt the new key and transmits the new group key to them.

The advantage of this approach is that the communication overhead is only one message for revoking any number of users. However, the number of keys stored by the VA and the users is exponential in the size of the group.

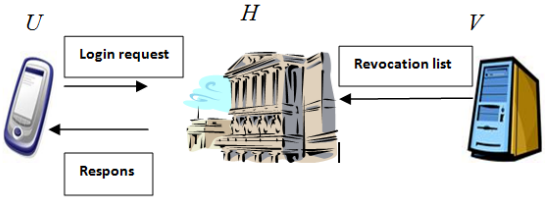

Figure 1. Overall design of the system

The enhancement is to evaluate trade-off between storage and revocation cost. Storage is computed in terms of keys that each user (respectively, VA) maintains. And revocation cost is computed in terms of the encryptions performed, and the number of messages transmitted, by the VA.

A. Creation of Wireless Communication Network

The wireless communication network is created by five steps they are as

Server :Server Side modules consists of VLR and HLR coding of each mobile stations and also modules for different network group.GSM subscribers use the mobile stations to make and receive calls. Mobile stations are the combinations of Subscriber Identity Mobile (SIM) and mobile equipment. Base Station (Visiting Location Register-VLR): Mobile Subscribers communicate with a base transceiver station (BTS) over radio interface. Base station generally takes the up-link radio signals from MS and converts it into data for transmission to other machines within the GSM network and vice versa.

GSM Operation Center (Home Location Register – HLR): The center is responsible for accepting mobile subscribers to the system, route the communications between mobile subscribers. HLR is a main database of subscriber information of the GSM operator. It interacts with mobile switching center, which is a center call and control processing

Client: Mobile Clients are more sensitive on computation time than PC's, their capacity is restricted both on memory and CPU and also usually their processors are using 16 bit architecture instead of 32 or 64 bit. The mobile client modules are implemented in Java.

B. Pre Authentication of Protocol

The implementation of pre-authentication of protocol between two devices that wish to communicate with each other at this or a later time[8]. In this phase either a secret key or an authentic copy of a public key are securely shared between the devices. Authentication delay plays an important factor in the overall handover delay[3]Keys can be shared during pre-authentication using the pre-authentication models

(1) VLR-GS. Keygen (N, T): The group manager runs this algorithm. This algorithm takes as input integers N, $T\epsilon\mathbb{N}$ indicating the number of subscribers (i.e., users) and the number of time intervals, respectively. Its output consists of a master public key mpk, a vector of N subscribers' secret keys $usk = (usk[1], \ldots, usk[N])$ and a vector of $N \times T$ revocation tokens $urt=(urt[1][1], \ldots, urt[1][T], urt[2][1], \ldots, urt[2][T], \ldots, urt[N][T])$, where $urt[i][j]$ denotes the revocation token of user Ui at time interval j.

(2) VLRGS. Sign (mpk, $[i]$, j,): This algorithm takes the master public key mpk, $u[i]$, the current time interval j and a message $M\epsilon\{0, 1\}^*$, and outputs a group signature σ.
The algorithm is as follows.

- Select random number $\alpha, \beta, \delta\ \epsilon_R Z^*_p$.
- Compute $T1 = A_i \tilde{} g^{\alpha}$, $T2 = g^{\alpha \tilde{} } g^{\beta}$, $T_3 = (g^{x_i}, h_j)$, and $T4 = g^{\delta}$.
- Compute $V = \{(\alpha, \beta, \delta, x_i,) : T1 = A_i \tilde{} g^{\alpha} \wedge T_2 = g^{\alpha \tilde{} } g^{\beta} \wedge T_3 = e(g^{x_i}, h_j)^{\delta} \wedge T_4 = g^{\delta} \wedge e(A_i, wg^{x_i}) = e(g, g)\}(M)$. For simplicity, the detailed description of the signature from zero-knowledge proofs of knowledge (SPK) is omitted in this paper.
- Output the group signature $\sigma = (T_1, T_2, T_3, T_4,)$.

(3) VLR-GS.Verify (mpk, j, RL_j, σ,): It takes as input mpk, the interval j, a set of revocation tokens RLj for interval j, a signature σ, and the message M. It outputs either "valid" or "invalid". The former output denotes that σ is a correct signature on M at interval j with respect to mpk, and the signer is not revoked at interval j.

This algorithm can perform two functions:

- Signature check. Check that σ is valid, by checking the
- Revocation check. Check that the signer is not revoked at interval j, by checking $T_3 \neq (T_4, B_{ij})$ for all $B_{ij} \in RL_j$.

C. User Join & Leave Mechanisms

A new user joining is about allowing a new user to register to a server after system setup. To support dynamic participation, an authentication scheme should support new user joining. For the above protocol, however, this new user joining mechanism no longer works. We assume a user U_n hopes to register to a server H during interval j_n. After

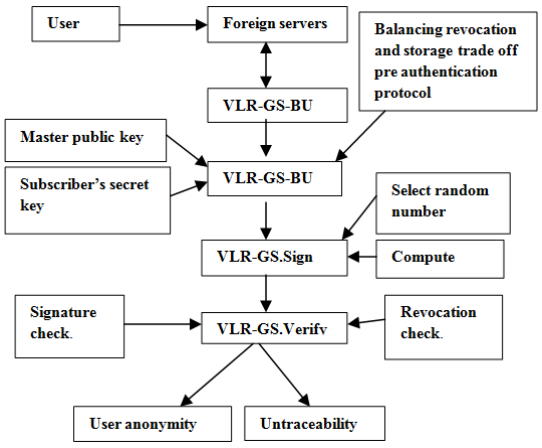

Figure 2. Overall design of the proposed system

verifying U_n's information, as the group manager of an independent VLR-GS-BU system,
H selects $x_n \epsilon_R Z^*_p$ and computes $A_n = g_1/(\gamma + x_n)$. After that, it computes $B_{nj} = h_{xn}\ j$ for all $j\epsilon[j_n, T]$. The master public key mpk is still $(g, \tilde{} g, h_1, \ldots, h_T, w)$. Un's secret key $[n]$ is (A_n, x_n). The revocation token at interval j of user Un is $[n][j] =$

B_{nj}, where $j \epsilon [j_n, T]$. The length of the master public key of H but also the number of revocation tokens is linear to . The master key of H is stored on every subscriber of H while the revocation tokens are stored on H.

D. Balancing Revocation and Storage Trade Off

The protocol VA needs to interrupt the communication during the rekeying; the resulting delay can be unreasonable for many applications. Thus, efficient distribution of the new key for multiple membership changes is a critical problem in secure group communication. One approach to revoke multiple users is to associate a key with every nonempty subset of users in the group. Thus, if one or more users are revoked, the VA uses the key associated with the subset of the remaining users to encrypt the new key and transmits the new group key to them. The advantage of this approach is that the communication overhead is only one message for revoking any number of users.

4. EXPERIMENTATION RESULTS

Fig3,4,5 shows the home location register, visitor location register and user. It also shows how it get stated using the port number and the local host by VLR-GS-BU algorithm. The user is login by the user name.

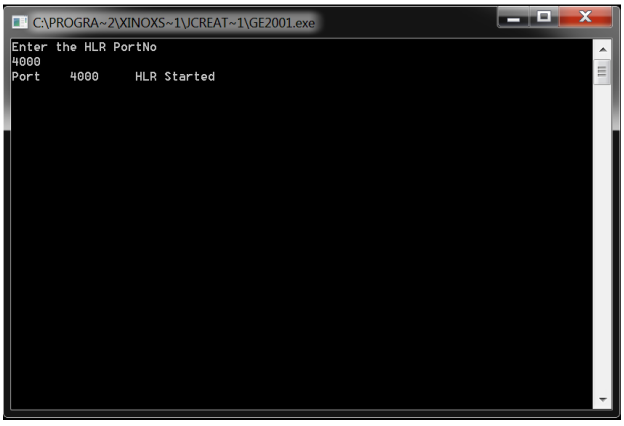

Figure 3. HLR image

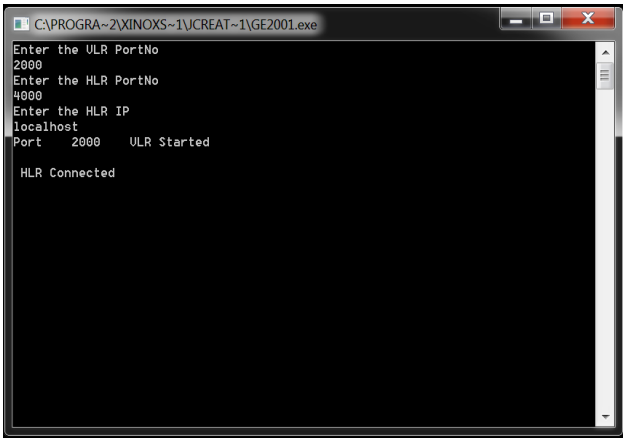

Figure 4. VLR image

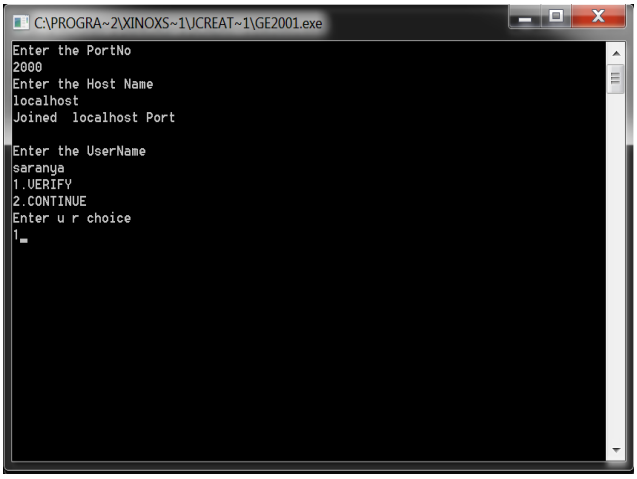

Figure 5. User login using VLR-GS-BU

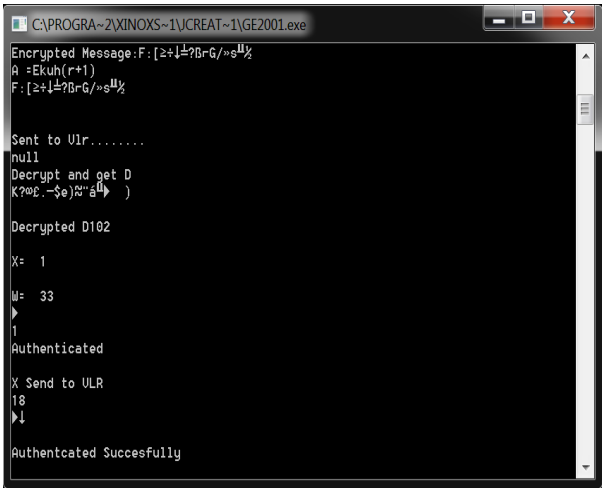

Figure 6. VLR-GS-BU verification

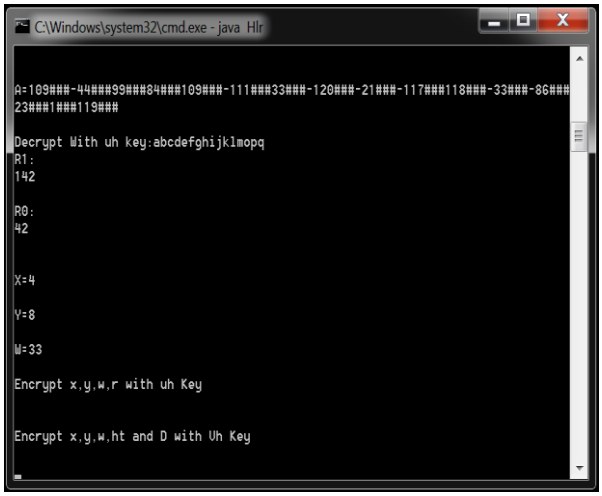

Figure 7. Key generated in HLR

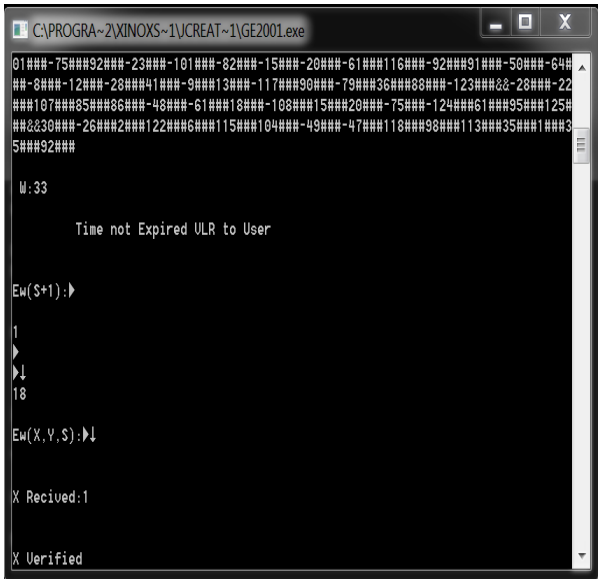

Figure 8. Key generated in VLR

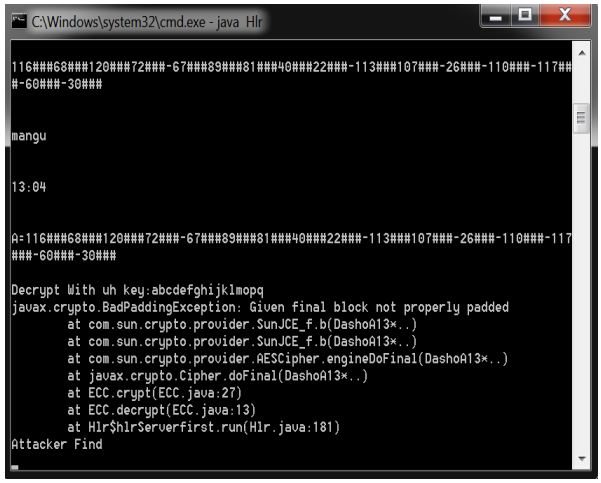

Figure 9. Attacker node

Fig6.shows the message authentication operations such as ECDSA Elliptic Curve Scalar Multiplication (ECSM) operation for signing, Multi-ECSM operation for verifications are very high. Fig7,8 shows key generated in the home location and visitor location and the session is also generated. For evaluating the effectiveness of proposed system we calculate key generation complexity for both systems and prove that proposed system is less complex than existing.

Table I
Comparsion between YHWD, YWD and Priauth

Protocols	Number of parties	Universal	Resistance to DOS attack	Perfect forward secrecy	User untraceability
YHWD	2	YES	NO	NO	NO
YWD	3	NO	NO	NO	YES
PRIAUTH	2	YES	YES	YES	YES

SSL specification, has been introduced into the implementation of Priauth. The same experiment is performed ten thousand times and average is taken over them. Table-I, shows the comparision between YHWD, YWD and Priauth We assume the access device of a roaming user runs on a 798 MHz processor, thus it takes 39.7 ms (plus 35.7 ms pre-computed). For new user joining, it just takes ($T - jn$+2) ECSM computations on H while the new user does not need to do any computations.

5. CONCLUSION & FUTURE WORK

The proposed a novel protocol to achieve privacy-preserving universal authentication for wireless communications. provide a trade-off between the number of keys maintained by the users and the time required for rekeying due to the revocation of multiple users. enables the group controller to deal with heterogeneous set of users that have different capabilities. With this capability, users with high capability can benefit from it (by reducing the rekeying cost), while users with low capability can still participate. We also showed that our algorithm can provide differential service to users that are long term versus those that are short term. We also demonstrated that our hierarchical algorithm can be combined with the logical key hierarchy in [3]. Such hybrid schemes provide additional options for the group controller to adapt to heterogeneous systems where users have varying requirements and capabilities.

6. REFERENCES

[1] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Commun., 2010, doi:10.1016/j.comcom.2010.02.031.

[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 168-174, 2010.

[3] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," IEEE Trans. Wireless Commun., vol. 6, no. 9, pp. 3461-3472, 2007.

[4] G. Yang, D. Wong, and X. Deng, "Deposit-case attack against secure roaming," in Proc. ACISP'05, 2005.

[5] D. He and S. Chan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," Wireless Personal Commun., 2010, doi: 10.1007/s11277-010-0033-5M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," IEEE Trans. Wireless Commun., vol. 4, no. 2, pp. 734-742, 2005.

[6] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," IEEE Trans. Consumer Electron., vol. 53, no. 5, pp. 1683-1687, 2006.

[7] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Commun. Lett. vol. 12, no. 10, pp. 722-723, 2008.

[8] J.-L. Tsai, "Efficient multi-server authentication scheme based on one way hash function without verification

table," Computers & Security, vol. 27, no. 3-4, pp. 115-121, 2008.

[9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. CRC Press LLC, 1997.

[10] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118-1123, 2009.

[11] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in Proc. ACM CCS'04, pp. 168-177, 2004.