GSM SECURITY II

Basar Kasim
Havelsan, Hava Elektronik Sanayi A.S
Eskisehir Yolu 7km
Ankara, Turkey
bkasim@havelsan.com.tr

Levent Ertaul
Department of Mathematics & Computer Science
California State University, East Bay,
Hayward, CA, USA.
levent.ertaul@csueastbay.edu

Abstract - *Mobility of users, transmission of signals through open-air, the requirement of low power consumption by mobile users and smaller data storage area limitation in mobile equipment make mobile wireless networks more vulnerable to security threats like eavesdropping and unauthorized access. This paper proposes a new set of security protocols to enhance the access and data security features of GSM mobile networks. These protocols are based on the Elliptic Curve Diffie-Hellman key agreement scheme and modified to be used in mobile environments.*

Keywords: GSM security, Wireless Security, Elliptic Curve Cryptology

1 Introduction

Mobile or wireless networks have become popular during the last ten years. They allow mobile users to make telephone calls, transfer/receive data while the users are on the move. On the other hand, wireless networks are more vulnerable to unauthorized access and eavesdropping when compared with the traditional fixed wired networks. This is mainly due to the mobility of users, the transmission of signals through open-air, the smaller storage areas and the requirement of low power consumption by the mobile users.

This paper focuses on the GSM (Group Special Mobile or System for mobile Communications) security system [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. In order to cover security weakness discussed in [12], a new set of protocols aimed to enhance the GSM security is proposed through the following sections.

The Elliptic Curve Cryptography (ECC) [15, 16, 17, 18, 19, 20, 21, 22] constitutes the major element of the protocols proposed. This is mainly due to the fact that, the Elliptic Curve Cryptosystems provide the highest strength per-bit of any cryptosystem known today. Reduction in key sizes brings the advantage of less storage area and less bandwidth, which are the important requirements of the wireless network architectures. In addition, the ECC permits the implementation of high-speed and efficient network security protocols requiring less power and smaller code sizes [20, 21, 22, 23, 24, 25].

2 New Elliptic Curve Cryptography Protocols for GSM Security

As described in [12], the current GSM security architecture and the proposed enhancements have so many security flaws. In order to cover these flaws, several protocols are proposed in the following sections. A relatively new public key cryptography technology, the EC Public Key Cryptosystem, is used in these protocols. The ECC permits the implementation of high-speed and efficient network security protocols requiring less power and smaller code sizes when compared with the classical public key techniques like RSA [26] and Diffie-Hellman (DH) [27].

2.1 Elliptic Curve Diffie-Hellman (ECDH)

The ECDH protocol (Figure 1) is used to produce a shared secret value (K_{UN}) between two communicating parties (e.g. the user and the GSM network) [17, 21, 19]. This secret value can then be used to distribute the content encryption key that encrypts sensitive data.

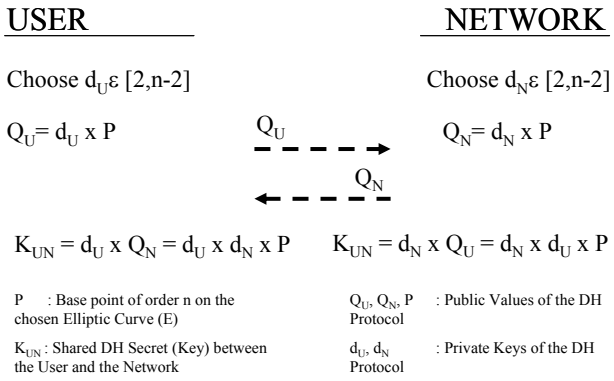

Figure 1 –ECDH Protocol

EC public keys of the communicating parties can be distributed by using Elliptic Curve (EC) digital certificates that contain the following fields [28]:

Issuer Identity: Identity of the certificate issuer, which is the user's home network.

Public Key of the User: ECDH public key Q_U.

Validity Period: User's certificate is valid within the time interval specified by this parameter.

Signature Field: Issuer's Elliptic Curve Digital Signature Algorithm (DSA) signature on the user's certificate [20, 21]. The signature is computed over the following fields: Issuer identity, user's identity, public key of the user, certificate validity period

User certificate does not contain the identity of the subscriber in explicit form; but id of the user is taken into account during the signature generation operation. Purpose of this process is to hide the user identity to prevent unauthorized persons to track the user by using the certificate exchanges. Network certificates can be prepared by a global certification authority trusted by all networks. Since there is no need to hide the identity of networks, network identifications can be placed in their certificates.

2.2 Local Authentication

After the registration of a mobile subscriber to a new domain, successive authentication operations on that user can be performed locally without communicating with the user's home network. This reduces the overhead on the home networks of those users. In these protocols, before the authentication phase begins, the mobile user and the visited network must have the each other's certificate.

2.2.1 Diffie-Hellman Key Agreement and Authentication

The ECDH secret value can be used to distribute the content encryption key between the visiting user and the visited network (Fig. 2) The GSM user and the network can also use this protocol to authenticate each other.

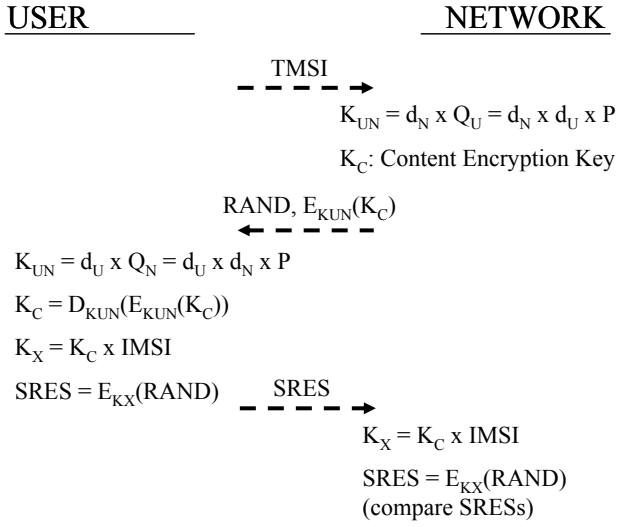

Figure 2 – EC Diffie Hellman

The protocol given in the Figure 2 uses a challenge response based authentication technique where the network's random number is the challenge of the network and the signed response is the response of the user [15]. The correct signed response could only be generated by the user, if that subscriber has the correct ECDH secret (K_{UN}) to decrypt the $E_{KUN}(K_C)$ expression. It can be seen that in the SRES expression $K_X=K_C$ x IMSI is used as the key to the encryption algorithm E. Purpose of this operation is to avoid the known plaintext attacks on the SRES - KC pair.

2.2.2 ECDH Key Agreement and Authentication II

The protocol given in the section 2.2.1 has some flaws: Anyone obtaining the random number RAND and the signed response SRES can use these values to obtain the content encryption key K_C, by using the input output relationships of the encryption algorithm E. Same argument is true for the DH secret K_{UN}. In order to solve these problems, Figure 3 is proposed.

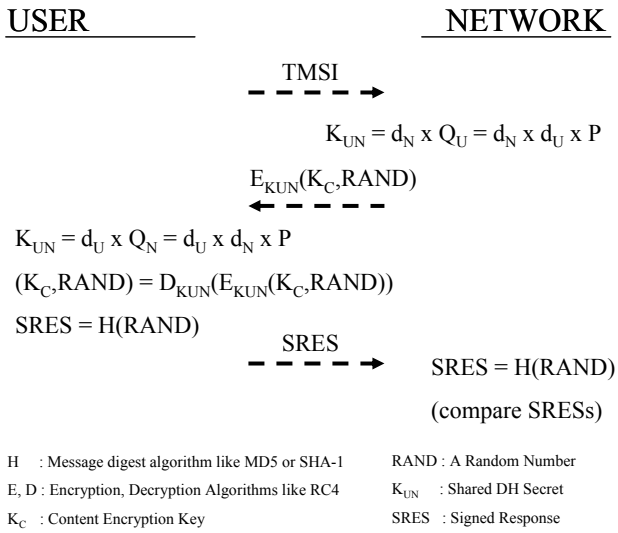

Figure 3 – ECDH Protocol II

In this protocol, the network does not send the random number (RAND) in clear; it is also encrypted with the shared DH secret. In addition, the signed response SRES is generated by using a message digest algorithm like SHA-1 [29]. Message digest algorithms are characterized by the fact that, it is computationally infeasible to find the input of the message digest or hash algorithm by using only its output.

2.2.3 Modified EC Diffie-Hellman

If the protocols given in the sections 2.2.1 and 2.2.2 are used, the DH secret (key - KUN), which is used to encrypt the content encryption key, will be the same for all the time. In order to eliminate this, ordinary ECDH authentication and key exchange protocol is modified as in the Figure 4:

1. The user generates the session key KC and the signed response by using the parameters sent by the network.

2. After receiving SRES and $d_U^{-1}.RAND_U$ from the user, the network generates the content encryption key as:

$K_C = Q_U \times ((d_U^{-1} .RAND_U).RAND_N) = P \times d_U ((d_U^{-1} .RAND_U).RAND_N) = P \times (RAND_N.RAND_U)$ (1)

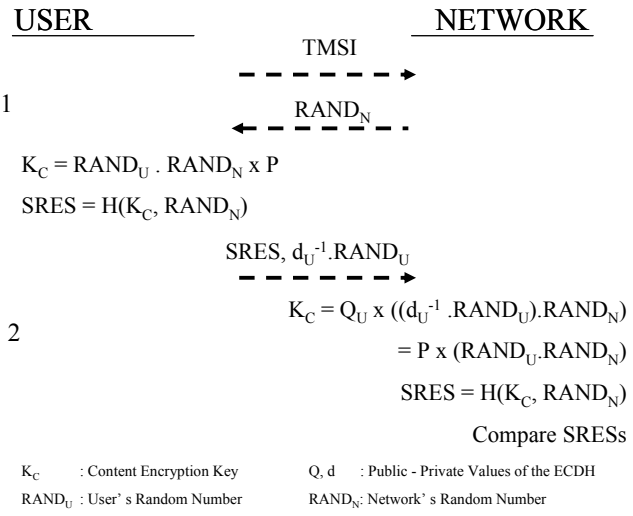

Figure 4 - Modified Diffie Hellman Protocol

d_U^{-1} is the inverse of d_U over the chosen elliptic curve group. The network calculates the Signed Response and compares it with the received SRES from the user. Since only the user's public key can generate the correct content key, a match in these SRES values authenticates the user to the network.

This protocol has some weak points: Since the user does not perform any authentication operation on the network, anyone having the public key of the user can impersonate valid GSM networks. Generation of the content encryption key depends on security parameters that are transmitted in plaintext form through the air interface. So, anyone listening the traffic between the user and the network can calculate the content encryption key K_C.

2.2.4 Modified Diffie-Hellman - II

The flaws of the protocol given in the section 2.2.3 could be solved if the generation of the content encryption key depends on private keys of both the user and the network (Fig. 5)

1. d_U^{-1}. $RAND_U$ and d_N^{-1}. $RAND_N$ products can be thought as the new public values of the DH protocol. In order to protect the privacy of the private values, the randomness of the random numbers used in this step must be guaranteed. Here RAND is the challenge to the mobile subscriber.

2. The user and the network generates the content encryption key as

$K_C = Q_N \times ((d_N^{-1} .RAND_N).RAND_U) = Q_U \times ((d_U^{-1} .RAND_U).RAND_N) = P \times (RAND_N.RAND_U)$ (2)

3. The network receives and compares the user's response to the challenge RAND (SRES) with the signed response calculated. A match in these values authenticates the user to the network. After the successful user authentication, the network and the mobile subscriber use the content encryption key (K_C) to encrypt the voice and the signaling data. It can be seen that, this protocol uses one key for authentication and data privacy.

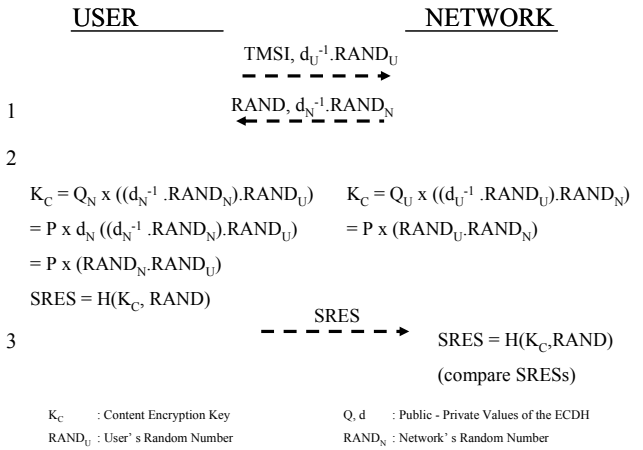

Figure 5 - Modified DH Protocol II

The local authentication protocols proposed for the GSM protects the user identity confidentiality by using temporary identities. Known and accepted private key encryption algorithms like AES [30] and RC4 [31] assure the user data and signaling element confidentiality on the air interface between the user and the GSM network. The visited networks use the EC digital certificates of the users to authenticate them. These public key based techniques make it possible to store the user specific secret keys only in the user SIM cards.

3 Conclusions

In this paper the security features of the current GSM architecture are examined and several EC public-key cryptography based protocols for the GSM security are proposed. Public key methods are chosen since these systems can easily be managed when key distribution is considered. Performance overheads of the public key cryptography are eliminated by not using the classical public key systems like Diffie-Hellman and RSA. Instead the ECC, which is characterized by efficiency both in key sizes and speed performance, are favored. In all protocols user authentication and the key distribution services are accomplished by using the public key cryptography methods whereas data encryption is performed by using the private key cryptography methods, which are more efficient than the public key methods when the speed performance is considered.

Use of the public key cryptography methods assures that mobile user's private parameters are stored only in their SIM cards. Public key certificates used in the proposed system do not contain the identity of their owners to satisfy

the user identity confidentiality on the air interface; but the digital signatures on these certificates take the user ids into account to assure the binding between the certificates and their owners.

Local authentication services allow the visited networks to authenticate the visiting users without consulting to the users' home networks. This reduces the network traffic and the computational overhead on the visited and the home networks. These local authentication protocols also provide a remote domain security mechanism having minimal impact on the user interface with respect to the home domain authentication process.

Besides the fact that, the designed security protocols are explained in the GSM environment, flexible design of these protocols makes it possible to use them in any wireless network architecture. In the future it is planned to simulate the designed protocols in computer environment to obtain the speed performance parameters.

4 References

[1] S.H. Redl, M.K. Weber, M.W. Oliphant, "An Introduction to GSM", Artech House, '95.

[2] J.Scourias, "Overview of the Global System for Mobile Communications", Waterloo Unv, Oct.'97

[3] D. Margrave, "GSM Security and Encryption", George Mason University.

[4] European Telecommunications Standards Institute (ETSI), "Dig. Cellular Telecommunications Sys. (Ph 2); Sec. Related Network Functions", GSM 03.20 v. 4.4.1.

[5] ETSI, "Digital Cellular Telecommunications System (Ph 2+); Security Aspects", GSM 02.09.

[6] ETSI, "Dig. Cellular Telecom. System (Ph 2+); Security Mngmt.", GSM 12.03 version 7.0.1 Release 1998.

[7] ETSI, "Dig. Cellular Telecom. System (Ph 2); Network Arch.", GSM 03.02, Third Edition, Nov.'96.

[8] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users", IEEE Network Mar./Apr.'94, pp. 26.

[9] C.S. Park, "On Certificate Based Security Protocols for Wireless Mobile Communication Systems", IEEE Network Sep./Oct.'97, pp. 50-55.

[10] C. Duraiappan, Y.Zheng, "Enhancing Security in GSM", Int. Computer Symp., Taiwan, Dec.'94.

[11] Basar Kasim, Levent Ertaul, "Evaluation of GSM Security", in Proceedings of the Fifth Symposium on Computer Networks (BAS 2000), Bilkent-Ankara / Turkey, June 2000, pp. 69-78.

[12] Basar Kasim and Levent Ertaul, "GSM Security", International Conference on Wireless Networks ICWN, Las Vegas, USA, 2005

[13] G. M. Koien, "An introduction to Access Security in UMTS", IEEE Wireless Communications, Vol.11, No 1, Feb.'04.

[14] G. Rose, G. M. Koien, "Access Security in CDMA2000 including a comparison with UMTS Access Security", IEEE Wireless Communications, Vol.11, No 1, Feb.'04.

[15] Bruce Schneier, "Applied Cryptography", Second Edition 1996, John Wiley & Sons.

[16] W. Stallings, "Network Security Essentials: Applications and Standards", 4th Ed. 2006, Prent.-Hall Inc.

[17] N. Koblitz, "Elliptic Curve Cryptosystems", Math. Of Computation, v. 48, 1987, pp. 203-209.

[18] Certicom Corporation, "The Elliptic Curve Cryptosytem for Smart Cards", May'98

[19] M. Aydos, E. Savaş and Ç. K. Koç, "Implementing Network Security Protocols based on the Elliptic Curve Cryptography" 4th Symp. on Comp. Networks, Turkey, May'99, pp.130-139,

[20] A. J. Menezes, D. B. Johnson, "Elliptic Curve DSA (ECDSA): An Enhanced DSA", Usenix Sec. Symp., San Antonio-Texas, Jan. ' 98, pp. 33-43.

[21] Certicom Corporation, "Certicom ECC Tutorials"

[22] Certicom Corporation, "Current Public-Key Cryptographic Systems", Apr. '97

[23] Certicom Corp., "Remarks on the Security of the Elliptic Curve Cryptosystem", July 2000

[24] K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, vol. 11, no. 1, pp. 62-67, Feb.'04

[25] A.K. Lenstra, E.R. Verheul, "Selecting Cryptographic Key Sizes", ECC 99, Nov.'99, Waterloo Canada,.

[26] R.L. Rivest, A. Shamir, L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. 21-n.2, February 1978, pp. 120-126.

[27] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov.'76, pp. 644-654.

[28] C.Adams, S.Lloyd, "Understanding Public Key Infrastructure", '99, Macmillan Tech. Publishing.

[29] R.L. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[30] D.J., Rijmen, V."Rijndel: The Advanced Encryption Standard", Dr. Dobb's Journal, Mar.'01.

[31] M. Robshaw "Stream Ciphers", RSA Labs Technical Report TR-701, July 1995