PROVIDING VOICE PRIVACY OVER PUBLIC SWITCHED TELEPHONE NETWORKS

[2]Mohamed Sharif and [1,2]Duminda Wijesekera
{msherif|dwijesek}@gmu.edu
[1]Center for Secure Information Systems,
[2]Department of Information and Software Engineering,
George Mason University, MS 4A4, Fairfax, VA 22030-4444

Abstract: The public telephone network has been evolving from manually switched wires carrying analog encoded voice of the 19th century to an automatically switched grid of copper-wired, fiber optical and radio linked portions carrying digitally encoded voice and other data. Simultaneously, as our security consciousness increases, so does our desire to keep our conversations private. Applied to the traffic traversing the globe on the public telephone network, privacy requires that our telephone companies provide us with a service whereby unintended third parties are unable to access other's information. However, existing public telephone network infrastructures do not provide such a service. This paper proposes a security architecture that provides end-to-end voice privacy and authentication services within the boundaries of the existing public telephone network infrastructures. Proposed architecture uses public key cryptography for authentication and key distribution, and symmetric key cryptography for voice privacy. This work is a part of an on going project on securing telecommunication system architectures and protocols.

Key words: Public Switched Telephone Network (PSTN), Signaling System 7 (SS7), Certificate Authority (CA), ANSI-41 (IS-41), Global System for Mobile Communications (GSM), Secure Telephone Unit Third Generation (STU III)

1 INTRODUCTION

Wired or wireless voice communication, otherwise known as telephony plays an important role in our society. By lifting the handset of the telephone and dialing a series of numbers we can reach any other telephone in the

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

world. However, as things stand today, an eavesdropper can easily monitor supposedly private telephone conversations. Thus, telephone calls need to be protected against eavesdropping. Existing security architectures in wire-line and wireless telephone infrastructures comes short of providing end-to-end voice privacy as well as authentication for subscribers. Thus, the main objective of this paper to describe an architecture that provides end-to-end voice privacy at the application layer with minimum modification to existing public telephone network infrastructures. Voice privacy is achieved by encrypting voice signals between two end telephones using symmetric keys and a one-time encryption key. This one-time encryption key is used to prevent replay attacks. We also propose imposing an authentication mechanism for telephone subscribers and telephones that are to be used for secure communications. Proposed authentication technique uses public key cryptography and provides authentication center(s) the assurance that the telephone set and the user at the other end of the connection are what they claim to be. We show how to integrate our proposed key distribution services on public telephone grids.

Our proposed architecture for secure telephony will be implemented at the *application service elements* (ASE) layer of the *Signal System 7 (SS7)* protocol model, where exiting security architectures and other advanced intelligent network services in the wire-line and wireless network are being implemented. Proposed architecture takes advantage of information sharing taking place between the telephone companies to facilitate wire-line and wireless call processing.

The rest of the paper is organized as follows. Section 2 summarizes related work involved with the security of wire-line and wireless telephone networks. Section 3 provides a detail description of the proposed security architecture. Section 4 describes how to integrate the proposed security architecture with PSTN. Finally, Section 7 concludes the paper.

2 RELATED WORK

Telephone services have been improving from old hand switched analog encoded telephones to current day advance intelligent network applications. However the security in wire-lines, otherwise known as *public switched telephone network* (PTSN) is still a major concern. Currently, PTSN does not have a system to protect against unauthorized eavesdropping of conversations. That is not to say there is no way to conduct secure telephone conversation in PSTN. There are several secure telephones that provide protection againt eavesdropping in PSTN. These secure telephones are design to work only as dedicated pairs through public telephone network infrastructure and use predetermined symmetric keys. In addition, most of these secure phones address only the confidentiality part of the security

services and not other security services such as authentication, authorization, and non-repudiation. An example of such a secure phone is STU III, discussed next.

2.1 Secure Telephone Unit: Third Generation (STU III)

Secure telephones widely used in the intelligence community, commonly known as *secure telephone unit third generation (STU III),* was developed by the National Security Agency (NSA) in 1987 [20]. It uses symmetric keys to encrypt voice messages. These keys are downloaded and stored in the telephone unit. STU III has an in-built key management system for customizing and downloading keys. Obtaining a STU III requires NSA's permission.

2.2 Wireless Networks

Wireless communications are more susceptible to eavesdropping than wire-line (Public Switch telephone Network) communication, because readily available radio scanners can easily monitor radio signals [6,19]. Because wireless signals are sent over the air using insecure radio channels, eavesdroppers can not only monitor the conversation but also obtain mobile station information such as Mobile Identification numbers. Once this information is known, it can be used to create a clone. Due to mobile station cloning, Wireless telephone industry is loosing millions of dollars every year [13,21]. In order to address these security issues, the wireless industry started to implement authentication to protect against cloning and confidentiality (voice privacy) to protect against eavesdropping.

Authentication and confidentiality for wireless network are defined in ANSI-41 (IS-41) and *Global System for Mobile Communications (GSM)* standards. Both IS-41 and GSM security are based on symmetric key cryptographic techniques where a secret key is shared between the mobile station and the authentication center in the network. Details of IS-41 and GSM security appear on [3,5,6,9]. Both IS-41 and GSM security addresses the issue of wireless telephone cloning, but do not offer end-to-end voice privacy or subscriber authentication.

3 PROPOSED SECURITY ARCHITECTURE

The proposed security architecture consists of *certificate authorities (CA), authentication centers (AC)* and telephone sets with cryptographic capabilities on top of the existing public telephone network infrastructure as shown in Figure 1.

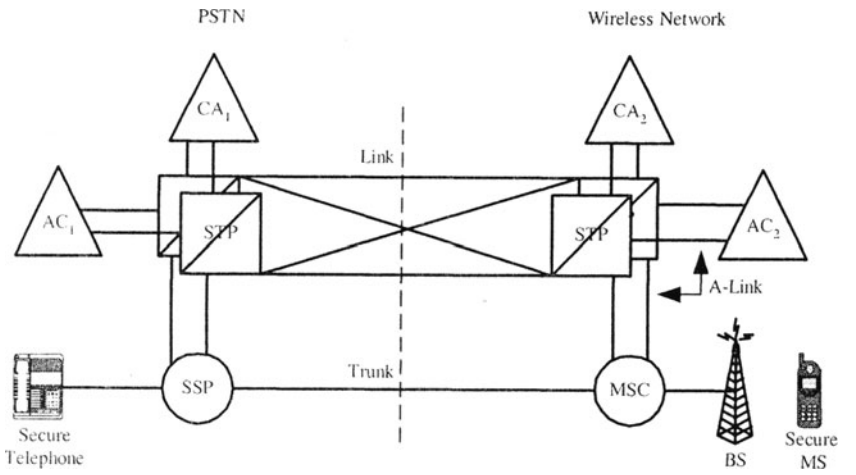

Figure 1. Secure Network Architecture

The CA and AC are to be implemented at the *application service element (ASE)* of the SS7 protocol model. CA is responsible for generating public/private keys, creating digital certificate of public keys, and storing the digital certificates in the publicly available database as well as interfacing with other CA's in the public telephone network. In addition, it is responsible for maintaining the *certificate revocation list (CRL)*, which contains the list of compromised and expired keys. A digital certificate is a record that binds the telephone's public key to the telephone number and is signed by the CA of the telephone company, which is providing the privacy services.

AC is responsible for generating and distributing the encryption keys, and authenticating telephones and subscribers. It is also responsible for maintaining the authentication database, which contains subscriber profiles. Subscriber's profile contains the subscriber identification with corresponding password as well as other information. AC interfaces with other AC's in the public telephone network to service roaming subscribers.

Proposed security enhancements assume that every telephone company establishes a *certificate authority (CA)* and every CA cross-certifies with other CA's in the telephone network. This cross-certification is only valid for the connection process, and allows a telephone or AC in one telephone company's domain to communicate securely with other telephones or AC's in a different telephone company's domain. We now describe authentication services in detail.

3.1 Authentication

The proposed security architecture uses public key cryptography to achieve authentication. The CA of the telephone company generates the public/private key pair and the digital certificate of the AC. It stores the digital certificate of the AC in the CA's database which is publicly available, and stores AC's public/private key pair in a secure file in the AC server.

Whenever a subscriber requests a telephone service, the CA generates the public/private key pair and a digital certificate of the telephone set. It stores the digital certificate of the telephone in the telephone's profile as well as in the CA's database. Then, the CA installs the telephone's public/private key pair and AC's public key in the telephone set. The telephone's profile contains other information in addition to public/private key pairs such as the telephone location, the subscriber, billing information etc. It can be stored in the *line information database (LIDB)* for PSTN telephones and in the *home location register (HLR)* for the wireless phone. The telephone's public/private key pair is unknown to the subscriber. When a private key of the telephone set is compromised, the CA will revoke the digital certificate of the telephone set and store it in the CRL as well as in the telephone's profile. Then it generates a new key pair.

When the subscriber requests privacy service, the subscriber will have to selects an ID and password pair, and the AC stores them in subscriber's profile. The subscriber's profile can be stored in the authentication database in the AC. A subscriber, who subscribes to the privacy service, can use any secure telephone to get voice privacy service. There are two types of authentication taking place in the proposed architecture: system (device) authentication and subscriber authentication. System authentication is used to authenticate the telephone set and the AC, and the subscriber authentication is used to authenticate the subscriber who is requesting a provicy service.

3.1.1 System Authentication

Either the telephone or the AC can initiate the system authentication and it is transparent to the subscriber. However, it will be mostly used by the AC to authenticate the telephone as illustrated in Figure 2. The following steps describe the telephone set authentication process:

1. The AC generates a random number (R), and it encrypts R with AC's private key (K^*AC) using the encryption algorithm (E) to obtain signed R (S_{AC}), which is the digital signature of the AC.
   [i.e. $S_{AC}=E_{K^*AC}(R)$].
2. The AC sends S_{AC} to the telephone set over the control channel of the digital subscriber lines and voice channel of the analog lines.
3. When the telephone set receives S_{AC}, it decrypts S_{AC} with AC's public key KAC using the decryption algorithm D to recover R,

[i.e. $R = D_{KAC}(S_{AC}) = D_{KAC}(E_{K*AC}(R))$].

4. The telephone set performs the same process as step 1 to sign the decrypted R, [i.e. $S_T = E_{K*T}(R)$], and then sends S_T to the AC.
5. When the AC receives S_T, it performs the same process as step 3 to decrypt the original R, [i.e. $R = D_{KT}(S_T) = D_{KT}(E_{K*T}(R))$]

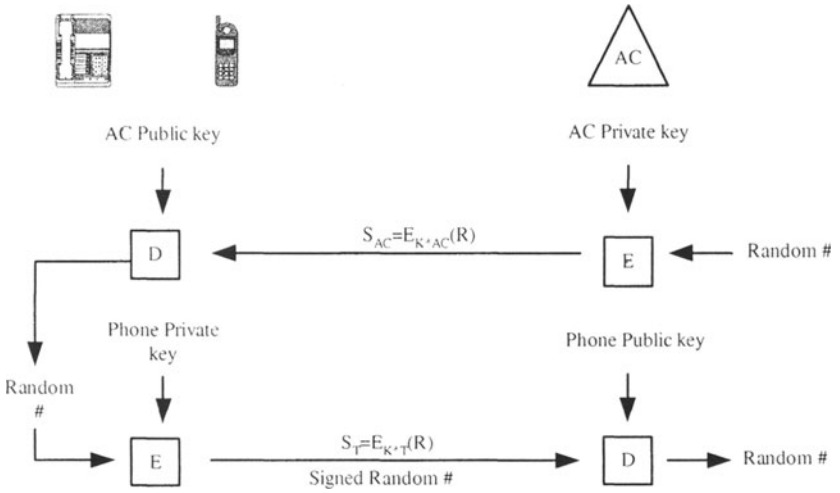

Figure 2. The System Authentication Process

This process provides the AC the assurance that the random number response came from the telephone. Now, the telephone set is allowed to receive services from the network.

3.1.2 Subscriber Authentication

When the caller requests a privacy service, the AC initiates the subscriber authentication process as illustrated in Figure 3, and The following steps describes subscriber authentication process:

1. The subscriber requests the secure connection, and in response, the *interactive voice response (IVR)* at the end office instruct the subscriber to enter the subscriber's ID and password (ID&P) pair over the voice channel.
2. Once the subscriber enters the ID&P, the telephone encrypts the ID&P with AC's public key (KAC) using the encryption algorithm E to obtain encrypted ID&P say C, [i.e. $C = E_{KAC}(ID\&P)$] and sends C to the AC over the control channel of the digital subscriber lines and voice channel of the analog lines.

3. When the AC receives C, it decrypts C with AC's private key K^*AC using the decryption algorithm D to recover *ID&P*, [i.e. $ID\&P = D_{K^*AC}(C) = D_{K^*AC}(E_{KAC}(ID\&P))$].

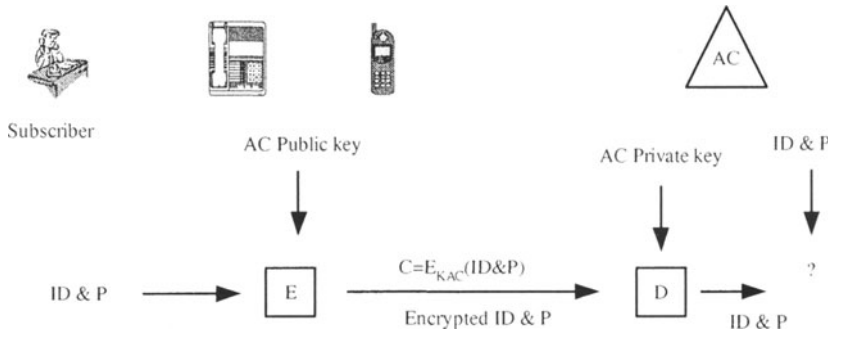

Figure 3. The Subscriber Authentication Process

The AC verifies the ID&P received with the ID&P in the authentication database. If verified to be correct, the calling subscriber is allowed to receive the privacy service, and is denied otherwise. Once the calling subscriber is authenticated, the AC authenticates the called subscriber using the same process.

3.2 Voice Privacy

Voice privacy is achieved by encrypting the voice signals between the two end telephones using a symmetric key algorithm as illustrate in Figure 4. Voice encryption starts when the telephone and subscriber are authenticated, at the caller's end and the called subscriber accepted the privacy service request. The following steps describes voice encryption process:

1. The AC generates the encryption key K_E, and encrypts it with the corresponding telephone's public key KMS using the encryption algorithm E to obtain encypted K_E, say C1 and C_2. Then, it sends C_1 and C_2 to telephone 1 (MS1) and telephone 2 (MS2) respectively over the control channel of the digital subscriber lines and voice channel of the analog lines. [i.e. $C_1 = E_{KMS1}(K_E)$, $C_2 = E_{KMS2}(K_E)$]
2. When each telephone set receives the encrypted K_E, it decrypts with its private key K^*MS using the decryption algorithm D to recover K_E, [i.e. $K_E = D_{K^*MS1}(C_1) = D_{K^*MS1}(E_{KMS1}(K_E))$], and uses it to encrypt/decrypt the voice signals using a *secret key encryption and decryption (E &D)*

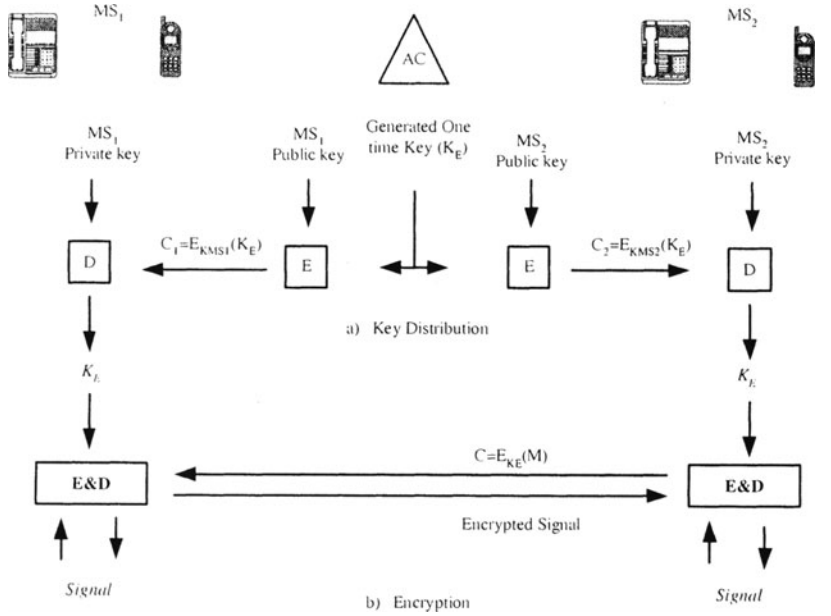

Figure 4. Voice Privacy in the Secure Architecture

This key K_E is only valid during the call in progress, and destroyed once the call is terminated.. If K_E is compromised during the call and the call is on an analog subscriber line the call must be disconnected. If K_E is compromised during the call and the call is on digital subscriber line, the AC will generate a new K_E and sends to the telephone over the control channel. Once the telephone receives the new key K_E, it destroys the compromised key and uses the new key. We are working on the process of compromised encryption key, and we will describe it in our next paper.

4 PROVIDING VOICE PRIVACY AS A SERVICE WITHIN THE PSTN

In PSTN, call processing involves setting up, monitoring, and releasing the connection as well as managing other features related to the call. The signaling protocol is responsible for the call processing. Figure 5 shows the typical signaling messages between two telephones on analog line in the PSTN. The signaling message between the telephone and *Sercvice Switching Point (SSP)* at the end office is subscriber signaling, and the signaling messages within the PSTN are *ISDN User Part (ISUP)* for connection setup and *Trasnaction Capabilities Applications Part (TCAP)* for features related

connection setup such as subscriber authentication, 800 number translation, etc. In Figure 5, the broken lines represent secure messages and solid lines represent normal messages. The following call process assumes that subscriber S_1 requests privacy call, S_2 accepts the privacy call, and S_2 hangs up first.

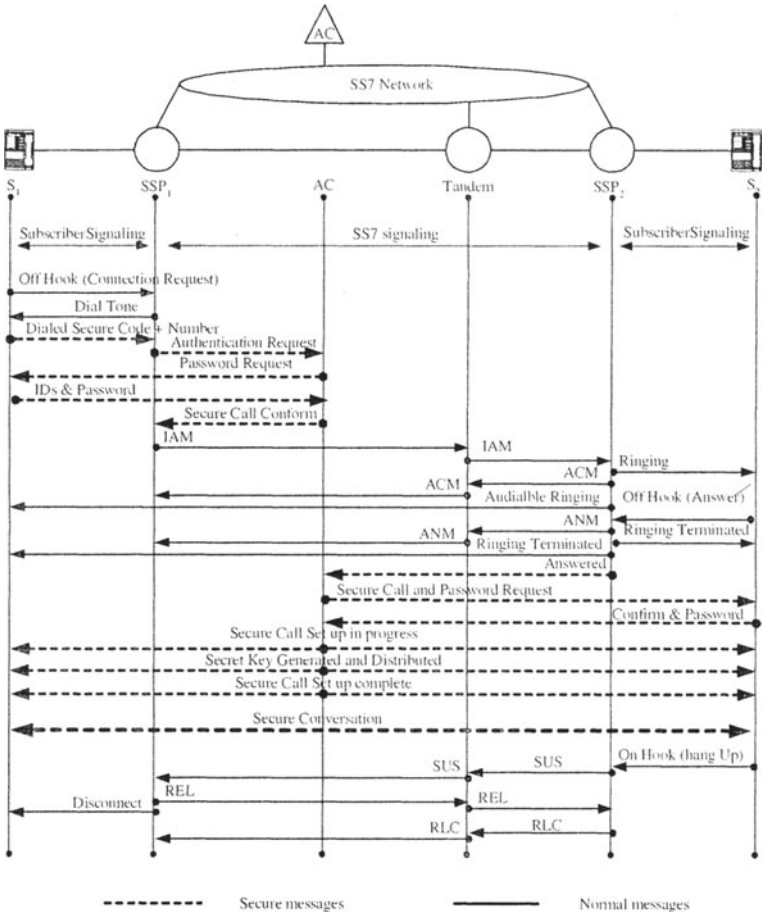

Figure 5. Typical Privacy Service Call Processing in PSTN

When S_1 lifts (Off-hook) the handset of the telephone, SSP_1 interprets off-hook as a request for service and responds with a dial tone to S_1. Then, S_1 dials the secure connection code and S_2's number. SSP_1 waits until all the numbers have been dialed and then examines and decides to route the call to the tandem, and to request for S_1's ID and password. Then, SSP_1 sends request for S_1's ID & password and S_2's ID to the S_1 via *interactive voice*

response (IVR) message. While SSP_1 is waiting the response from S_1, it identifies an available trunk, and sends *Initial Address Message (IAM)* to the tandem via SS7 network. IAM is an ISUP message and contains the information required for the tandem to setup the requested connection. Once SSP_1 receives the encrypted S_1's ID, S_1's password, and S_2's ID from S_1, it forwards it to the authentication center (AC) using an appropriate TCAP message. The connection process continues, If and only if the AC authenticates the S_1.

When the tandem receives the IAM, it examines the IAM and determines that it needs to forward the request to SSP_2. The tandem identifies an available trunk, generates another IAM, and sends it to SSP_2 via the SS7 network. When SSP_2 receives the IAM, it examines the IAM, and determines the status of S_2. If S_2 is busy, it sends a R*elease (REL)* message to SSP_1 via SS7 and releases the trunk for another call. REL is another ISUP message. Upon receiving the REL, SSP_1 sends a busy signal to S_1. However, if S_2 is available, SSP_2 sends *Address Complete Message (ACM)* to the tandem via the SS7 network, and the tandem forwards it to SSP_1. The ACM is an ISUP message, and informs SSP_1 that SSP_2 is ringing the S_2 and the requested trunk is reserved. SSP_2 sends the ringing tone to S_2 and S_1 through the trunk.

When S_2 answers the telephone, SSP_2 sends an *Answer (ANM)* message to the tandem, and a TCAP message to AC via the SS7 network. The ANM is an ISUP message that informs SSP_1 that S_2 has answered the call. When the tandem received the ANM, it sets up the forward path of the trunk between the tandem and SSP_2, and forwards the ANM message to SSP_1. Upon the receipt of ANM, SSP_1 sets up the forward path of the trunk between itself and the tandem. Finally, SSP_2 stops sending the ringing tone to S_1. The AC sends the privacy service and ID & password request to S_2 via IVR. If S_2 does not accept it or responds with incorrect ID & password, then S_1 is given a choice to continue as a normal connection or to terminate the connection. If S_2 responds with correct ID & password, then the AC announces the key generation and distribution (for detail, see previous section). Once S_1 and S_2 receive the encryption/decryption key, the secure conversation between S_1 and S_2 starts.

Figure 5 assumes that S_2 hangs up first and then SSP_2 generates and sends a *Suspend (SUS)* message to the tandem, which forwards it to SSP_1. When SSP_1 receives the SUS message, it starts a SUS timer and waits to receive an on-hook signal from S_1, a R*esume (RES)* message from SSP_2, or the SUS timer to expire. If a RES message arrives from SSP_2, the connection continues to be active. If an on-hook signal arrives from S_1 or the SUS timer expires, SSP_1 destroys the encryption key, sends a *Release (REL)* message to the tandem via the SS7 network, and releases the trunk. Upon the receipt of the REL message, the tandem releases the trunk, and sends a REL message to SSP_2 via SS7 network. When the SSP_2 receives the REL message, it destroys the encryption key and sends a *Release Complete (RCL)* message to the SSP_1

through the tandem. The RCL message means that the SSP_2 has released the trunk at its end.

5 CONCLUSIONS

We have described an architectural enhancement necessary to provide end-to-end voice privacy at the application layer of the SS7 protocol model with minimum modification to existing public telephone networks. Voice privacy is achieved by encrypting voice signals between the two end telephones using a symmetric key algorithm and one-time encryption key. The latter key is used to prevent replay attacks. In addition, we have described an authentication process for subscribers and telephones. The authentication techniques provide the AC the assurance that the telephone set and the subscriber at the other end of the connection are what they claim to be. Finally, we described how to integrate our proposed voice privacy service with the PSTN and wireless network. Our ongoing work addresses performance issues and an efficient PKI infrastructure suitable for the SS7 network. The summary of the comparison between the proposed security architecture and the existing security architectures in public telephone network is given in Table 1.

Table 1. Comparison between the proposed and existing security architectures

	Proposed Security Architecture	IS-41 Security	GSM Security	STU III [20]
Devices Authentication	Yes	Yes	Yes	No
Subscriber Authentication	**Yes**	**No**	**No**	**No**
Voice Privacy between the telephone and SSP or MSC	Yes	Yes	Yes	Not Applicable
End-to-End Voice Privacy	**Yes**	**No**	**No**	**Yes**
One time encryption key	Yes	Not Always	Not Always	Not Always

NOTES

This research is partly supported by NSF under grant CCR-0113515, Center for Secure Information Systems at GMU and Prof. S. Jajodia

REFERENCES

1. Berman, R. K. and Brewster, J. H., "Perspective on the AIN Architecture", IEEE Communications Magazine, 31, No. 2, February 1992.
2. Black, U., "ISDN and SS7", Prentice Hall PTR, Upper Saddle River, New Jersey, 1997.
3. Bosse, J. G. von, "Signaling IN Telecommunication Networks", John Wiley & Sons, New York, 1998.
4. Baum, M. S. and Ford, W., "Secure Electronic Commerce", Prentice Hall PTR, Upper Saddle River, New Jersey, 1997.
5. Carne, E. B., "Telecommunications Primer, Second Edition", Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.
6. Chlamtac, I., and Lin, Y., "Wireless and Mobile Network Architectures", John Wiley & Sons, New York, 2001.
7. Chow, M., "Understanding Telecommunications: Systems, Networks and Applications", Volume 1, Andan Publisher, Holmdel, New Jersey, 2000.
8. Douskalis, B., "IP Telephony", Prentice Hall PTR, Upper Saddle River, New Jersey, 2000.
9. Gallagher, M. D. and Snyder, R. A., "Wireless Telecommunications Networking with ANSI-41", Second Edition, McGraw-Hill, New York, 2001.
10. Modarressi, A. R., and Skoog, R. A., "Signaling System No. 7: A Tutorial", IEEE Communications Magazine, pp. 19-35, July 1990.
11. Noll, A. M., "Introduction to Telephones and Telephone Systems", Third Edition, Artech House, Boston, 1998.
12. Rappaport, T. S., "Wireless Communications", Prentice Hall PTR, Upper Saddle River, New Jersey, 2002.
13. Rose, G., "Authentication and Security in Mobile Phones", http://people.qualcomm.com/ggr/QC/AUUG99AuthSec.pdf
14. Russell, T., "Signaling System # 7", Second Edition, McGraw-Hill, New York, 1998.
15. Schneier, B., "Applied Cryptography", Second Edition, John Wiley & Sons, New York, 1996.
16. Scourias, J., "Overview of the Global System for Mobile Communications", http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html.
17. Stallings, W., "ISDN: An Introduction", Macmillan Publishing Company, New York, 1989.
18. Stallings, W., "Cryptography and Network Security", Second Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.
19. Tanenbaum, A. S., "Computer Networks" third Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 1996.
20. Department of Defense Security Institute, "STU-III Handbook for Industry", http://www.tscm.com/STUIIIhandbook.html, February 1997.
21. ISAAC security research group, "GSM Cloning", http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html, http://www.isaac.cs.berkeley.edu/isaac/gsm.html.