2002

Providing Secure Communication Services on the Public Telephone Network Infrastructures

Sharif, Mohamed; Wijesekera, Duminda; Michael, Bret

Providing Secure Communication Services on the Public Telephone Network Infrastructures*

[2]Mohamed Sharif, [1,2]Duminda Wijesekera and [3]J. Bret Michael
{msherif|dwijesek}@gmu.edu, bmichael@nps.navy.mil
[1]Center for Secure Information Systems,
[2]Department of Information and Software Engineering,
George Mason University, MS 4A4, Fairfax, VA 22030.
[3]Department of Computer Science,
Naval Postgraduate School, Mail Code: CS/Mj Monterey, CA 93943.

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 data. However, existing public telephone network infrastructures do not provide such a service. This paper shows a method to enhance the PSTN call processing model to provide end-to-end voice privacy and access control services within the boundaries of the existing public telephone network infrastructures. Proposed enhancement uses public and symmetric key cryptography. 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), Public key cryptography, Symmetric key cryptography, Certificate Authority (CA), ANSI-41 (IS-41), Global System for Mobile Communications (GSM), Secure Telephone Unit Third Generation (STU III), Voice Privacy.

* Partly supported by NSF under grant CCR-0113515, Center for Secure Information Systems at GMU and Prof. S. Jajodia.

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 numbers, we can reach any other telephone in the 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 access control for subscribers. Thus, the main objective of this paper to describe architecture that provides end-to-end voice privacy at the application layer with minimum modification of 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 access control mechanism for telephone subscribers and telephones that will be used for secure communications. Proposed authentication technique uses public key cryptography and provides authentication center the assurance that the telephone at the other end of the connection is what it claims to be. We will also show how to integrate proposed key distribution services on public telephone grids.

Our proposed security enhancement 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 enhancement 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. In order to make this paper self-contained, Section 3 provides a brief overview of SS7. Section 4 provides a detail description of the proposed security enhancement. Sections 5 describe how to integrate the proposed security enhancement into call processing model. Finally, Section 6 concludes the paper.

2 Related Work

Telephone services have been improving from old humanly 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 from 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 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 [29]. It is uses symmetric keys to encrypt voice messages. These keys are downloaded and stored in the handheld 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 [12,28]. 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 industry is loosing millions of dollars every year [22,30]. In order to address these security issues, 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 [8,10,12,16]. 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 Signaling Architecture of the PSTN

Signaling architecture is responsible for transferring control signals between components of the telephone network. These control signals establish, maintain, release connections, and facilitate other managerial and bookkeeping functions such as accessing relevant telephone network databases (described shortly). Such signaling has been evolving since early days of manual switching of the 19th century. Presently, there are two kinds of signaling techniques that are used in the telephone network: Channel-associated (in-band) and Common-channel (out-of-band) signaling. There are two types of common-channel signaling: built-in separate channel and separate channel signaling. In built-in separate channel signaling, the signaling protocol is carried on separate channel on the same trunk that carries the voice signals. Examples of built-in separate channel signaling are the D channel of ISDN networks. In separate channel signaling, the signaling protocol is carried on a separate network. An example of separate channel signaling is signaling system 7 (SS7).

3.1 Signaling System 7

Signaling System 7 (SS7) is an out-of-band signaling standard for the telephone network developed by ITU-TS, and defines the architecture and the protocols of signaling network. It is the signaling systems used in PSTN. In order to make this paper self contained, the next section provides a brief overview of SS7, but details of SS7 appear in standard references such as [7,8,23].

3.1.1 The Signaling Network

The signaling network is a separate network that carries the signaling messages between the SS7 components. There are three main components in PSTN: Service Switching Point (SSP), Signaling Transfer Point (STP), and

Service Control Point (SCP). These components are arranged throughout the SS7 network in such way that the network provides the maximum performance, reliability, and flexibility. A simplified design of signaling network is shown in Figure 1. Every SSP is connected to at least two STPs for reliability, and this design is known as a mated STP pair. A mated STP pair in one company is inter-connected with other mated STP pair of other companies. In addition, mated STP pair in one company can support SSPs of other companies. Every STP is connected to at least one SCP.

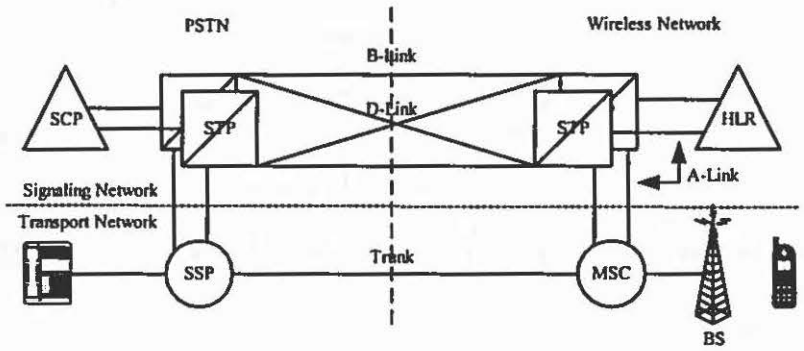


Figure 1. The Transport and Signaling Network in Public Telephone Network

SSP is a part of the local switch, which connects the telephone to the telephone network, and it is responsible for processing regular and special calls that require remote database translation. SSP also provides support to back-office functions such as configuration, billing, performance, error reporting, etc. An SSP in a wireless network is referred as a mobile-switched center (MSC). STP performs routing, and is responsible for routing signaling messages from its local SSP to destinations in the SS7 network. SCP is a process with access to the intelligent network (IN) database, and is responsible for processing requests from the SSP and other SCPs in the network. STP transfers these requests and responses to/from SCPs. Every database provide services specific applications such as subscriber profile, mobile station profile, 800 number translations, security, calling card and other services. Some of the commonly used databases are *line information database* (LIDB), *home location register* (HLR), Authentication, and *call management service database* (CMSDB).

3.1.2 Signaling Protocol

The SS7 protocol consists of a four-level hierarchy. This arrangement is similar to the four-layer hierarchy of the TCP/IP protocol model for data communication, as shown in Figure 3. Following is a short description of the SS7 protocol levels:

The Message Transfer Part (MTP) provides reliable transport of signaling messages across the SS7 network. MTP consists of the following three levels:

- MTP 1: Signaling Data Link corresponds to the lower half of network access layer of the TCP/IP protocol model, and defines the physical and other functional characteristics of the signaling links.
- MTP 2: Signaling Link corresponds to the upper half of the network access layer of the TCP/IP protocol model, and provides reliable transfer of signaling messages between signaling point.
- MTP 3: Signaling Network corresponds to the lower half of Internet layer of the TCP/IP protocol model, and provides routing functionalities.

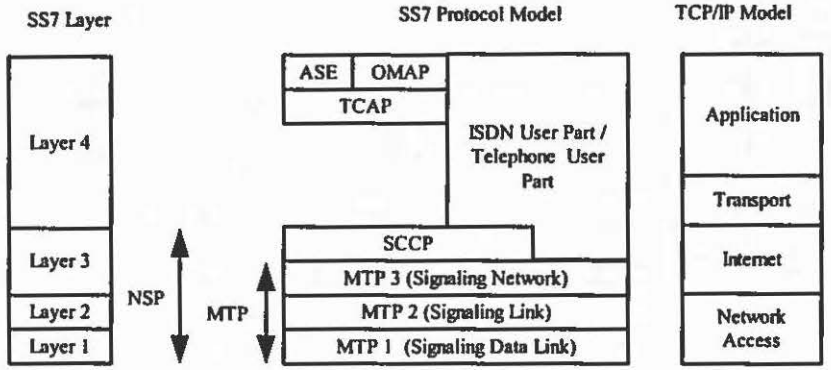


Figure 2. SS7 Protocol Model and TCP/IP Model

Signaling Connection Control Part (SCCP) corresponds to the upper half of the Internet layer of the TCP/IP protocol model, and provides functions to transfer non-trunk related messages such as database access. SCCP enhances the MTP 3 services by providing connectionless and connection-oriented classes of services. The combination of MTP and SCCP is known as the Network Services Part (NSP) of SS7.

Telephone User Part (TUP) is a protocol that provides call control, trunk maintenance, and call setup resources to the telephone network.

ISDN User Part (ISUP) is a protocol that provides call control, trunk maintenance, and call setup resources to the telephone network and the ISDN. North America uses ISUP and the rest of the world uses the TUP.

Transaction Capabilities Application Part (TCAP) is a connectionless remote procedure call (RPC) that allows one signaling point to invoke an operation to another signaling point and then use the response. It operates at the application of OSI protocol model, and provides a standard interface to the application service elements (ASE).

The Operation, Maintenance, and administration part (OMAP) is an application of TCAP and it provides the operations required to monitor, coordinate, and control of the telephone network.

The Application Service Element (ASE) is an application of TCAP. It is user specific services such as Mobile application Part (MAP).

4 Proposed Security Enhancement

The proposed security enhancement consists of certificate authorities (CA), authentication centers (AC) and telephone with cryptographic capabilities on top of the existing public telephone network infrastructure as shown in Figure 3. 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 device's public key to the device's identity and is signed by the CA. Digital certificate usually contains other information beside public key and identification, as defined in ITU-T Recommendation X.509 v3.

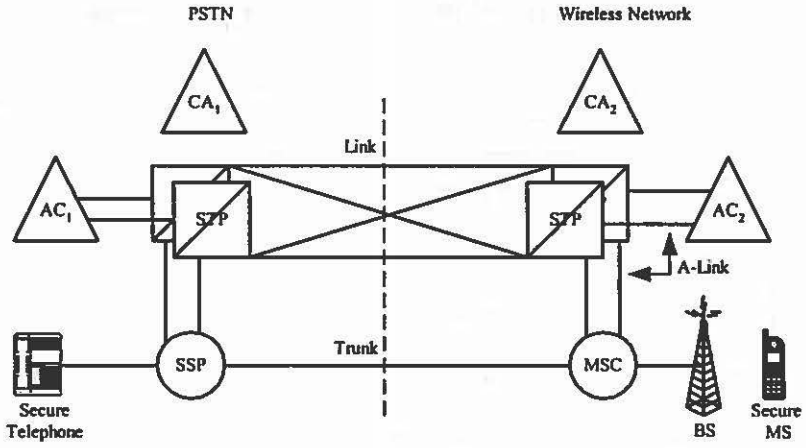


Figure 3. Secure Network Architecture

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 the subscriber 's profiles. Subscriber profile contains the subscriber identification and its corresponding requested password as well as other information related to subscriber. 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 connection process, and allows a telephone or AC in a 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.

4.1 Authentication

Proposed security enhancement uses public key cryptography to achieve authentication and key distribution. The public key cryptography uses public/private key pair. The private key is a secret key and is only known by its

owner, while the public key is publicly available. CA generates the public/private key pair and the digital certificate of AC. It stores the digital certificate of AC in a publicly available database, 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. It stores the digital certificate of the telephone in the telephone profile as well as a publicly available database. Then, the CA installs the telephone's public/private key pair and CA's digital certificate in the telephone at the telephone company. The telephone profile contains other information in addition to public/private key pairs. It can be stored in line information database (LIDB) for PSTN telephones and in home location register (HLR) for the wireless phone. The subscriber does not know the telephone's public/private key pair. When a private key is compromised, the CA will revoke it and store it in a CRL as well as in the telephone profile. Then it generates a new key pair.

At the time of the secure service request, the subscriber will have to selects one ID and password pair, and the AC stores them in subscriber profile. The subscriber profile can be stored in the authentication database that resides in the AC. A subscriber, who subscribes to the secure service, can use any secure telephone to get voice privacy. There are two types of authentication in the secure architecture: system (device) authentication and subscriber authentication. System authentication is used to authenticate the telephone and the AC, and the subscriber authentication is used to authenticate the subscriber who requested the secure connection.

4.1.1 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 4 (a). The following steps describe telephone authentication technique:

1. 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}), [i.e. $S_{AC}=E_{K^{*}AC}(R)$].
2. The AC sends S_{AC} to the telephone over the control channel for the digital subscriber line and voice channel for the analog line.
3. When the telephone receives S_{AC}, it decrypts S_{AC} with AC's public key (K_{AC}) using the decryption algorithm (D) to recover R, [i.e. $R = D_{KAC}(S_{AC})=D_{KAC}(E_{K^{*}AC}(R))$].
4. The telephone performs the same technique 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 technique as step 3 to decrypt the original R, [i.e. $R = D_{KT}(S_T)= D_{KT}(E_{K^{*}T}(R))$].

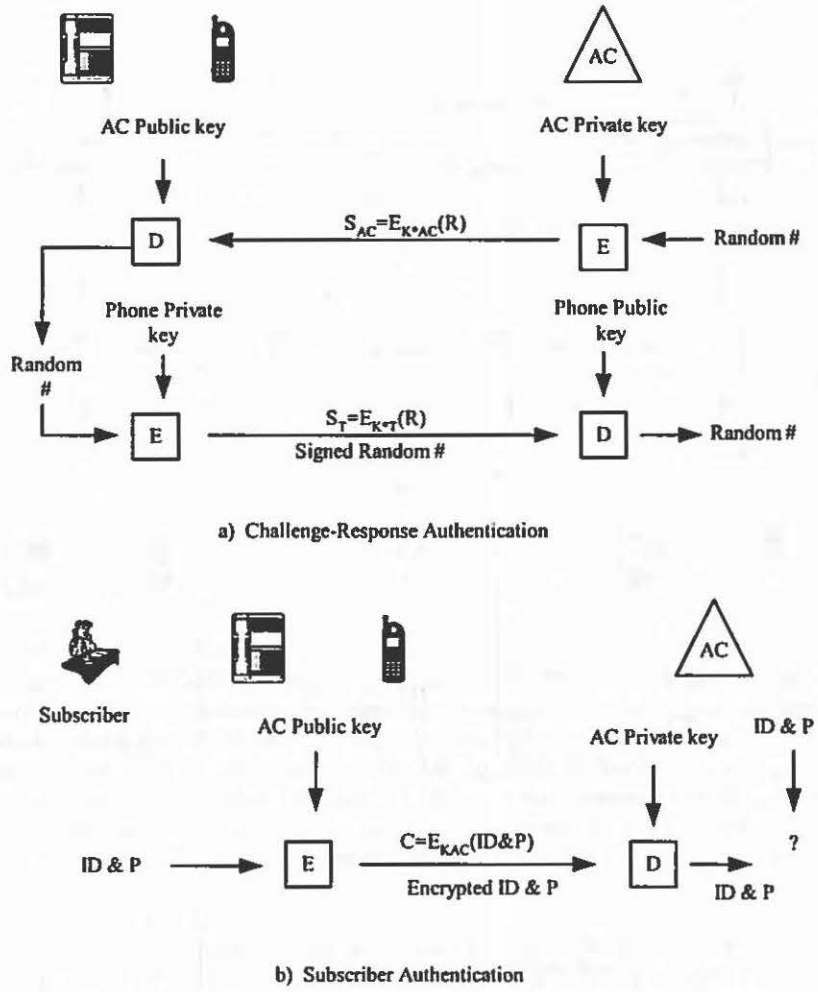


Figure 4. Authentication Techniques in Secure Architecture

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

4.1.2 Subscriber Authentication

When the calling subscriber requests secure connection, the AC initiates the subscriber authentication as illustrate in Figure 4(b). The following steps describes subscriber authentication:

- 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.
- Once the subscriber enters the ID&P, the telephone encrypts the ID&P with AC's public key (K_{AC}) 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 digital subscriber lines and voice channel of analog lines.
- When the AC receives C, it decrypts C with AC's private ($K^{\bullet}_{AC}$) using the decryption algorithm D to recover *ID&P*, [i.e. $ID\&P = D_{K^{\bullet}AC}(C) = D_{K^{\bullet}AC}(E_{KAC}(ID\&P))$].

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 a secure connection. Otherwise, the subscriber is denied a secure connection. Once the calling subscriber is authenticated, the AC authenticates the called subscriber using the same steps as those described in this section (4.1.2).

4.2 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 5. Voice encryption starts when the telephone and calling subscriber are authenticated, and the called subscriber accepted the secure connection request. The following steps describes voice encryption:

- The AC generates encryption key K_E, and it encrypts K_E with the corresponding telephone's public key K using the encryption algorithm E to obtain encrypted K_E called C, [i.e. $C = E_K(K_E)$]. It sends C to the telephones over the control channel for the digital subscriber line and voice channel for the analog line.
- When the telephone receives C, it decrypts C with telephone's private key $K^{\bullet}$ using the decryption algorithm D to recover K_E, [i.e. $K_E = D_{K^{\bullet}}(C) = D_{K^{\bullet}}(E_K(K_E))$], and uses it to encrypt/decrypt the voice signals using a secret key algorithm E & D

Key K_E is only valid during the call in progress, and once the call is terminated, the key is destroyed. There is no restriction on the key size, and it depends on the encryption algorithm. If the K_E is compromised during the call and the call is on 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.

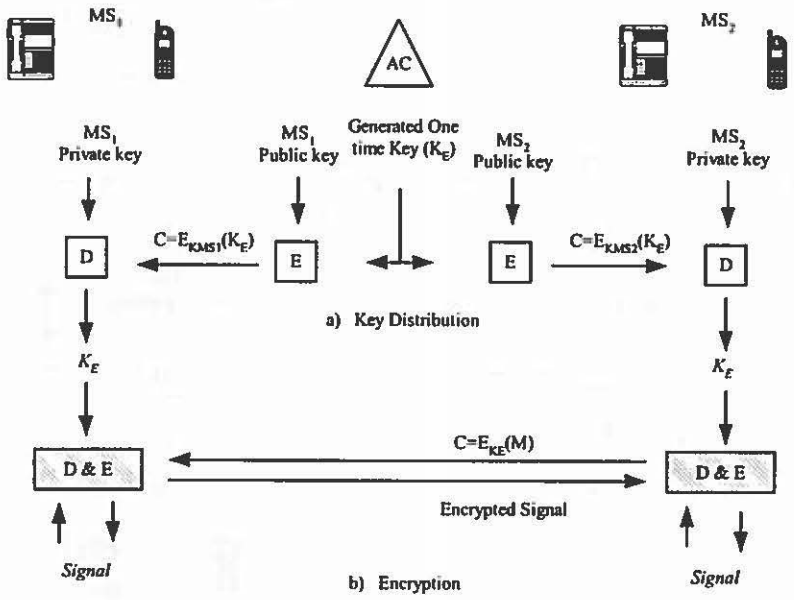
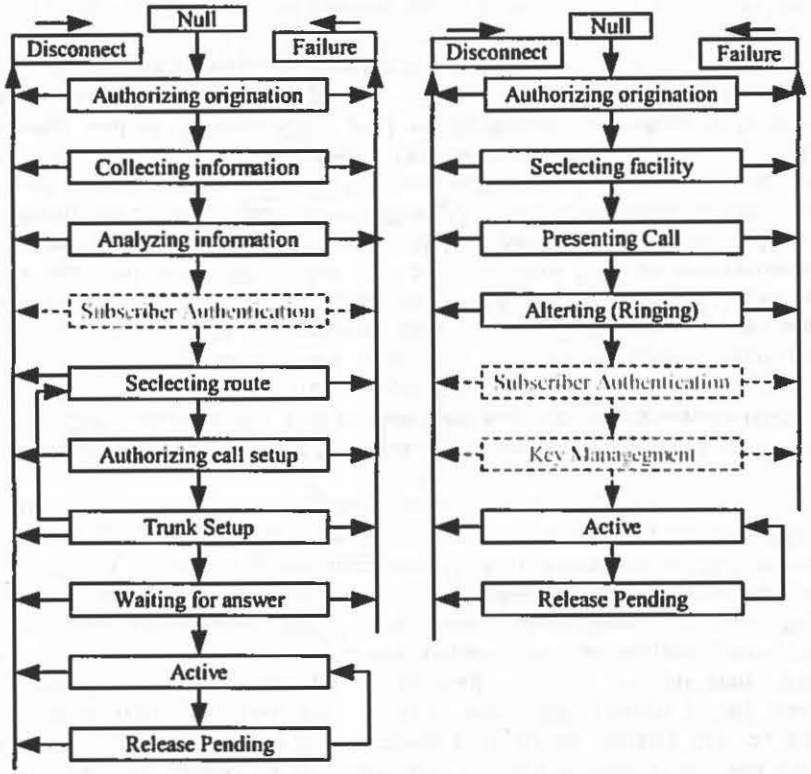


Figure 5. Voice Privacy in the Secure Architecture

5 Integrating Proposed Security Enhancement into the PSTN Call Processing Model

In PSTN, call processing involves setting up, monitoring, and releasing the connection as well as managing other features related to the call. As described in section 3, the signaling protocol is responsible for the call processing. The basic call-processing model (BCM) comprises into originating and terminating call processing [5,7,15].



a) Originating Basic Call model b) Terminating Basic Call model

Figure 6. Call-Processing Model with Proposed Enhancements

A simplified BCM with the proposed security enhancement states is shown in Figure 6 and the proposed states are shown in broken rectangular edges. The originating call-processing model (OCM) defines states for call processing related to the calling subscriber, and consists of ten original states and one proposed security enhancement state as shown in Figure 6. The termination call-processing model (TCM) defines states for call processing related to the called subscriber, and consists of seven original states and two proposed security enhancement states as shown in Figure 6. Each state in OCM and TCM represent a sequence of actions that SSP needs to perform at that point in processing the call. For all or some of the states, SSP may launch a query (initiate a transaction with) the service control point (SCP) or other devices such as authentication center (AC), etc, to receive instruction on how to handle the call at that point. When SSP initiates a transaction with SCP, SSP suspends the call processing and moves into wait state.

The mechanism, which SSP initiates a transaction with SCP through its local STP to obtain instruction to process the call, is referred as triggering. The mechanism, which SCP responds to the trigger, is referred as call-handling instruction. BCM uses TCAP messages and typical TCAP message flow between SSP and SCP is shown in Figure 7.

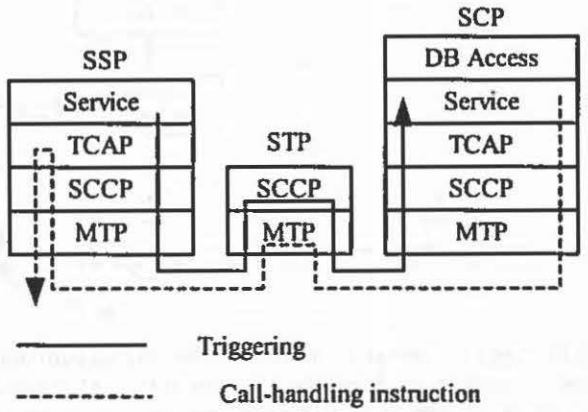


Figure 7. Typical TCAP message flow

The aforementioned provides a brief overview of the basic call-processing model and we now provide detail description of the proposed security enhancement states in BCM as shown in Figure 8, 9, and 10. In Figure 8, S_1 lifts (Off-hook) the handset of the telephone, the call process starts, and SSP_1 responds with a dial tone to S_1, and moves from null to colleting state. S_1 dials the secure connection code and the S_2 number. SSP_1 collects all the dialed numbers from S_1 and then moves to analyzing state. In this state, SSP_1 encounters subscriber authentication request and it initiates subscriber authentication transaction with AC to obtain call-handling instruction. Then SSP_1 moves to wait state where it waits the response from AC. In response, AC sends "send to resource, caller interaction (STR-I)" instruction to SSP_1, moves to wait state where it stays until the response from SSP_1 arrives. SRT-I instruction indicates that AC needs to interact with S_1.

When SSP_1 receives STR-I instruction, it moves to caller interaction state where SSP_1 connects S_1's line to intelligent-network service circuit (INSC), which plays the authentication announcement. The authentication announcement instructs S_1 to enter the password digits. INSC collects the password digits and SSP_1 sends them to AC in a resource clear message. SSP_1 moves to wait state and it stays there until a new instruction from AC arrives. When AC receives S_1's password from SSP_1, it retrieves S_1's password from the authentication database, compares it with the received S_1's password from SSP_1. If AC authenticates S_1, AC sends authenticated (AUTH-SUB) message to SSP_1, and moves to wait state. In response, SSP_1 moves from wait to selecting route state to continue the secure call processing. Otherwise, AC sends disconnect (DISC) message and in response SSP_1, goes to disconnect state where SSP_1 plays termination announcement. Termination announcement requests S1 to hung up because S1 is not authorize to make the call.

Figure 9 assumes that the call step up has been completed and S_2 has lifted the handset of the telephone. When S_2 answers the telephone, SSP_2 initiates subscriber authentication transaction with AC, and SSP_2 moves to wait state. In response, AC sends STR-I instruction to SSP_2, and moves to wait state where it stays until the response from SSP_1 arrives. Upon the receipt of STR-I instruction, SSP_2 moves to caller interaction state, and connects S_2's line INSC, which plays the authentication announcement, and collects the password digits. Then SSP_2 sends the password to AC, and moves to wait state. When AC receives S_2's password from SSP_2, it compares with the one in the authentication database. If the two passwords do not match, AC sends disconnect (DISC) message to SSP_1 and SSP_2. In response, Both SSP_1 and SSP_2 move to disconnect state where they plays termination announcement. Otherwise, AC sends secure call instruction to both SSP_1 and SSP_2, and moves to moves to key management state. Upon the receipt secure call instruction, both SSP_1 and SSP_2 move to secure call state where they play secure call announcement to S_1 and S_2. In key management state, AC generates, encrypts with corresponding the telephone's public key, and distributes one-time encryption key to both telephone via SSP_1 and SSP_2.

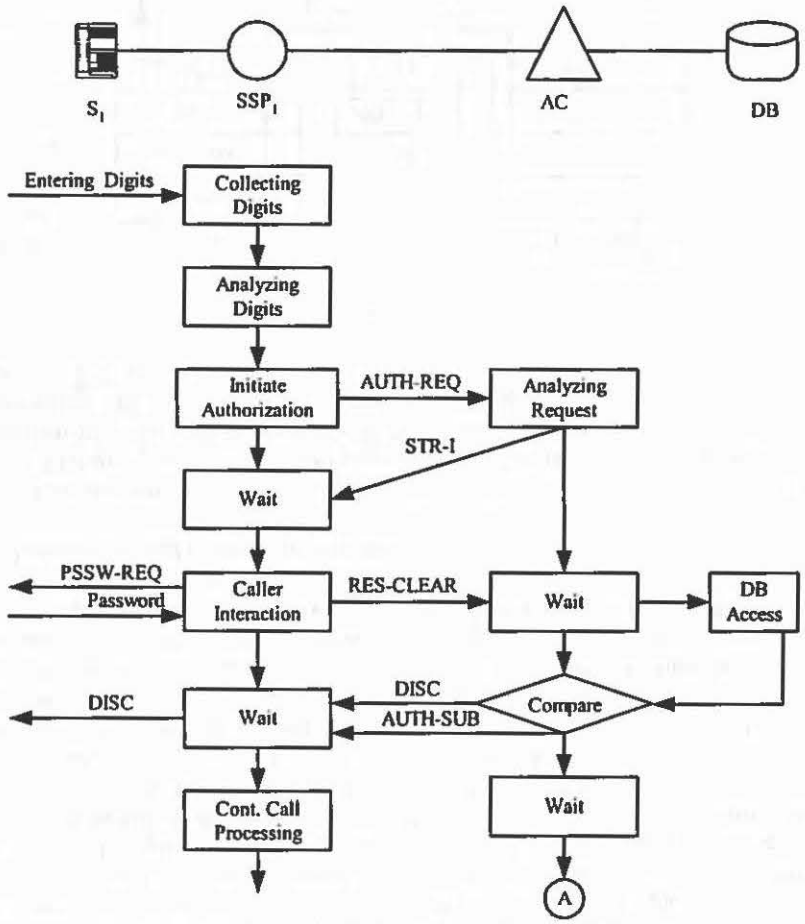


Figure 8. Originating a Secure Call

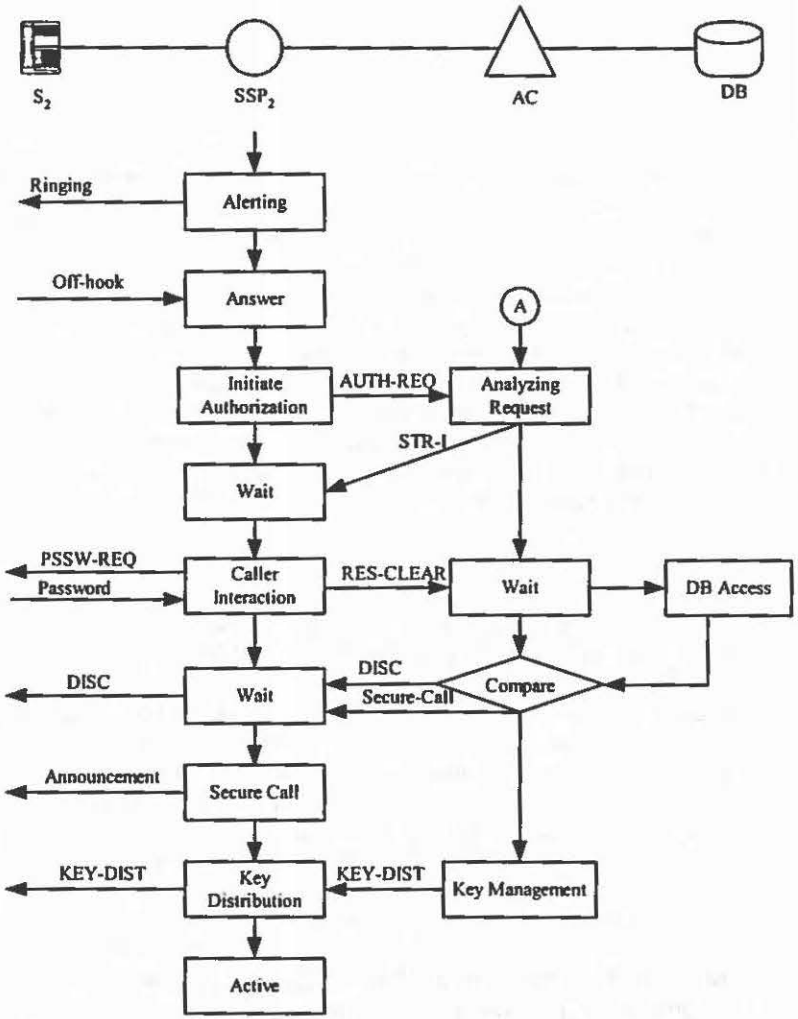


Figure 9. Terminating a Secure Call

Figure 10 illustrates a simplified secure call set up between telephones (S_1 and S_2) on analog line in the PSTN. In order to distinguish secure and normal message, we used the broken lines to represent secure messages and solid lines to represent normal messages. The steps of the simplified secure call set up shown in Figure 10 is as follows:

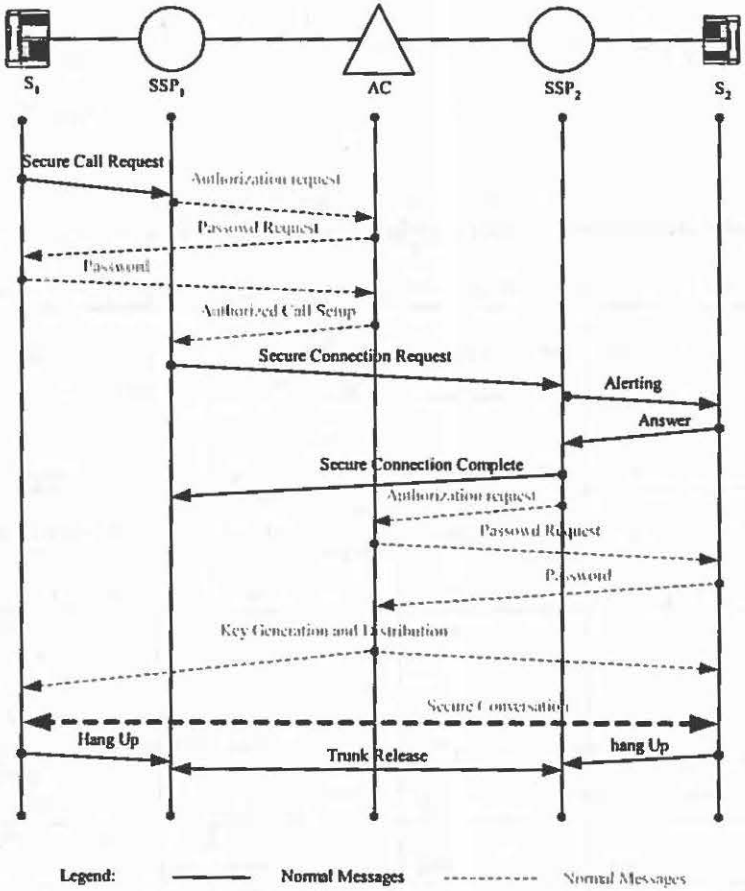


Figure 10. Simplified Secure Call Set up

1 S_1 dials the secure connection code and the S_2 number and SSP_1 collects all the numbers. SSP_1 examines the dialed numbers and send authorization message to AC.

2 AC sends request for ID & password to S_1 via interactive voice response (IVR), and then evaluates the received ID and password. AC instructs SSP_1 to continue secure call setup if S_1 is authenticated. Otherwise AC instructs $SSP_1$to disconnect the call.

3 SSP_1 identifies an available trunk and send secure connection request to SSP_2.

4 SSP_2 examines the received message from SSP_1, and alerts S_2.

5 Once S_2 answers, SSP_2 send connection complete message to SSP_1 and sends authorization request to AC.

6 AC sends request for password to S_2 via interactive voice response (IVR), and then evaluates the received ID and password. AC generates and distributes encryption key if S2 is authenticated. Otherwise, AC instructs SSP_1 and SSP2 to disconnect the call.

7 S1 and S2 use the encryption key to encrypt and decrypt the voice signal. When the connection is released, the encryption key is destroyed.

6 Conclusions

We have described an architectural enhancement necessary to provide end-to-end voice privacy at the application layer 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 keys. One-time encryption key is used to prevent replay attacks. In addition, we have described authentication techniques for subscribers and telephones. Telephone authentication technique provides AC the assurance that the telephone at the other end of the connection is what it claims to be. Finally, we described how to integrate voice privacy technique with PSTN and wireless network. Our ongoing work addresses performance issues and an efficient PKI infrastructure over SS7. The summary of the comparison between the proposed security enhancement and the most widely used security architectures in telephony is given in table 1.

	Proposed security enhancement	IS-41 Security	GSM Security
Devices Authentication	Yes	Yes	Yes
Subscriber Authentication	Yes	No	No
Voice Privacy between the telephone and SSP or MSC	Yes	Yes	Yes
End-to-End Voice Privacy	Yes	No	No
One time encryption key	Yes	Not Always	Not Always
Device Authentication Technique	Digital Signature	MAC	MAC
Subscriber Authentication Technique	Public Key Cryptography	Not Available	Not Available
Voice Privacy Technique	Secret Key Cryptography	Combination of MAC and "XOR"	Secret Key Encryption

(MAC is stand for message authentication code and XOR is stand for exclusive or)

Table 1. Comparison between the proposed security enhancement and existing security architectures

References

1. Ambrosch, W. A, Maher, A., and Sasscer, B., "The Intelligent Network", Springer-Verlag, New York, 1989.
2. Amoroso, E., "Fundamentals of Computer Security Technology", Prentice Hall PTR, Upper Saddle River, New Jersey, 1994.
3. Ash, G., "Dynamic Routing in Telecommunications Networks", McGraw-Hill, New York, 1998.
4. Bates, B., and Gregory, D., "Voice and Data Communications Handbook", McGraw-Hill, New York, 1996.

5. Berman, R. K. and Brewster, J. H., "Perspective on the AIN Architecture", IEEE Communications Magazine, 31, No. 2, February 1992.
6. Black, U., "Internet Telephony", Prentice Hall PTR, Upper Saddle River, New Jersey, 2001.
7. Black, U., "ISDN and SS7", Prentice Hall PTR, Upper Saddle River, New Jersey, 1997.
8. Bosse, J. G. von, "Signaling IN Telecommunication Networks", John Wiley & Sons, New York, 1998.
9. Baum, M. S. and Ford, W., "Secure Electronic Commerce", Prentice Hall PTR, Upper Saddle River, New Jersey, 1997.
10. Carne, E. B., "Telecommunications Primer, Second Edition", Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.
11. Chan, W. C., "Performance Analysis of Telecommunications and Local Area Networks", Kluwer Academic Publishers, Boston, 2000.
12. Chlamtac, I., and Lin, Y., "Wireless and Mobile Network Architectures", John Wiley & Sons, New York, 2001.
13. Chow, M., "Understanding Telecommunications: Systems, Networks and Applications", Volume 1, Andan Publisher, Holmdel, New Jersey, 2000.
14. Cole, M., "Introduction to Telecommunications", Prentice Hall PTR, Upper Saddle River, New Jersey, 2000.
15. Douskalis, B., "IP Telephony", Prentice Hall PTR, Upper Saddle River, New Jersey, 2000.
16. Gallagher, M. D. and Snyder, R. A., "Wireless Telecommunications Networking with ANSI-41", Second Edition, McGraw-Hill, New York, 2001.
17. Geier, J., "Wireless Networking Handbook", New Riders Publishing, Indianapolis, Indiana, 1996.
18. Kaufman, C., Perlman, R. and Speciner, M., "Network Security", Prentice Hall PTR, Upper Saddle River, New Jersey, 1995.
19. Nenezes, A. J., Oorschot, P. C. von, and Vanstone, S. A., "Handbook of Applied Cryptography", CRC Press LLC, New York, 1997.
20. Noll, A. M., "Introduction to Telephones and Telephone Systems", Third Edition, Artech House, Boston, 1998.
21. Rappaport, T. S., "Wireless Communications", Prentice Hall PTR, Upper Saddle River, New Jersey, 2002.
22. Rose, G., "Authentication and Security in Mobile Phones", http://people.qualcomm.com/ggr/QC/AUUG99AuthSec.pdf
23. Russell, T., "Signaling System # 7", Second Edition, McGraw-Hill, New York, 1998.
24. Schneier, B., "Applied Cryptography", Second Edition, John Wiley & Sons, New York, 1996.
25. Scourias, J., "Overview of the Global System for Mobile Communications", http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html.
26. Stallings, W., "ISDN: An Introduction", Macmillan Publishing Company, New York, 1989.
27. Stallings, W., "Cryptography and Network Security", Second Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 1999.
28. Tanenbaum, A. S., "Computer Networks" third Edition, Prentice Hall PTR, Upper Saddle River, New Jersey, 1996.
29. Department of Defense Security Institute, "STU-III Handbook for Industry", http://www.tscm.com/STUIIIhandbook.html, February 1997.
30. 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.
31. "SS7 overview", http://www.ss8.com.
32. "TR45.3 Appendix A to IS-54 Rev. B", http://islab.oregonstate.edu/documents/products/cave.html
33. "The GSM Security Technical White paper for 2002", http://www.hackcanada.com/blackcrawl/radiophone/assorted/gsm_security.html.

Biographies

Mohamed Sharif is currently pursuing PhD degree at George Mason University, and his areas of research are telecommunication and computer security. He holds BS in Electrical Engineering and Mathematics, and MS in Electrical Engineering from University of Maryland.

Duminda Wijesekera is an assistant professor of Information and Software Engineering at George Mason University. His areas of research are Computer Security and Formal methods. He holds PhD degrees in Computer Science and Mathematics from the University of Minnesota and Cornell University respectively.

J. Bret Michael has been an Associate Professor of Computer Science at the Naval Postgraduate School since 1998. His most recent research on the subject of distributed computing has been focused on issues pertaining to information security, system architecture, and software system safety. Prior to joining NPS, he conducted research at the University of California at Berkeley on the technical feasibility of fully automating the operation of dual-mode passenger and commercial vehicles on limited-access highways. He received his Ph.D. degree from George Mason University's School of Information Technology and Engineering in 1993.

Proceedings of the

Tenth International Conference on Telecommunication Systems

Modeling and Analysis

October 3-6, 2002
Monterey, California

VOLUME ONE

Sponsors

American Telecommunications Systems Management Association

IFIP Working Group 7.3

INFORMS Technical Section on Telecommunications

INFORMS Information Systems Society

Naval Postgraduate School, Monterey, CA

School of Management, The University of Texas at Dallas

World Scientific and Engineering Society