26

Design of Secure End-to-End Protocols for Mobile Systems

V. Varadharajan and Y. Mu
Department of Computing, University of Western Sydney, Nepean,
PO Box 10, Kingswood, NSW 2747, Australia

Telephone: +61 47 360192, Fax: +61 47 360 800
Email: vijay@st.nepean.uws.edu.au

Abstract

Use of mobile personal computers in open networked environment is revolutionalising the way we use computers. Mobile networked computing is raising important security and privacy issues. This paper is concerned with the design of authentication protocols for a mobile networked computing environment. We propose secure end-to-end protocols between mobile users using a combination of public key and symmetric key based systems. These protocols enable mutual authentication and establish a shared secret key between mobile users. They also provide a certain degree of anonymity of the communicating users to other system users.

Keywords

Authentication Protocols, Mobile Security, Hybrid Approach, Anonymity

1 Introduction

Information and communication technology is on the threshold of new style of computing (Cox, 90). First, the telecommunications industry is witnessing the development of Personal Communication Systems that are "person-specific" with person to person logical connections. Such systems rely more and more on wireless communications, both in the fields of voice and data communications between mobile personal computers and computer systems. Second, the computer industry is in the phase of practical implementation of distributed systems concept. In particular, the notion of open systems is a major driving force. Whereas today's first generation notebook computers and personal digital assistants are self-contained, networked mobile computers are part of a greater computing infrastructure. This raises several issues with regard to information security and privacy, system dependability and availability (Varadharajan, 95; Molva, 94).

J. L. Encarnação et al. (eds.), *Mobile Communications*

The paper is organised as follows. We begin in Section 2 by outlining the mobile computing environment. Section 3 gives the security requirements that need to be addressed in the design of the protocols. Section 4 proposes both intra and inter domain end-to-end protocols which can be used to provide authentication of mobile users. We use a hybrid approach involving both symmetric key and public key based systems. The design of protocols using only the symmetric key approach has been considered in (Varadharajan, 96). Finally, Section 5 discusses the important characteristics of the proposed protocol.

2 Mobile Environment

A simple mobile computing environment is shown in Figure 1. Mobile Computing Stations (MS) access the mobile network via a mobile network system. For instance, the network system may consist of Base Stations, Location Register, and Mobile Switching Component. The Location Register contains information related to the location and the subscription of the users in its domain. We will assume that an Authentication Server is present in every domain. This is logically a distinct entity; in practice, it may be co-located with the Location Register. The Authentication Servers store confidential information such as keys and are assumed to be physically protected. The mobile stations can move from one place to another, either within its domain (referred to as the "home" domain or move outside its home domain to a "visiting" domain. We will collectively refer to the authorities in the home domain as H and the authorities in the visiting domain as V.

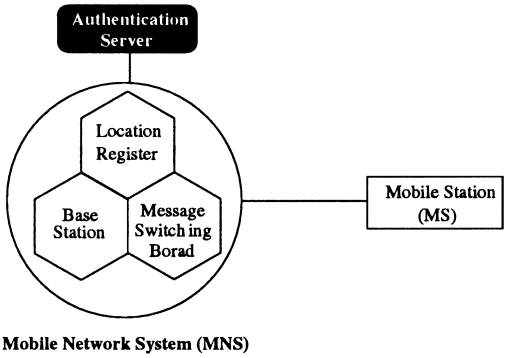

Figure 1: Mobile Networked Computing Environment.

We assume that when accessing the network in the home domain, the mobile user is authenticated with a server-based authentication mechanism. Users of every network domain are registered with that domain's authentication server. The authentication server of a domain can be replicated or partitioned within the domain but the set of all partitioned and duplicated authentication servers represent a single domain-level authority.

We will assume that users share a long term secret key with their home domain, i.e., A in domain H shares a secret key K_{AH} with H and B in domain V shares a secret key

K_{BV} with V. Authentication between domains is achieved using public key cryptography. That is, H and V have public key and private key pairs. When A travels to the visiting domain V, a shared session key between A and V must be established. In this paper, the user and the mobile computing station are regarded as an intact part.

3 Security Requirements

- *Authentication* : The authentication service should provide to the communicating parties the confidence that at the time of request, an entity is not attempting to masquerade as another and is not mounting a reply attack. In a secure mobile system, this implies that the end parties A and B should be confident that they are in fact communicating with each other. In order to achieve this, they rely on the guarantee provided by the Authentication Servers in their respective domains. That is, the mobile stations and the users of a domain trust both the competency and the honesty of their Authentication Server. For the Authentication Servers to be able to offer this guarantee, they need first to be able to reliably verify the identity of the communicating parties. Authentication between domain servers is achieved using a public key system.

- *Secure Communication* : The communication should not be vulnerable to attacks from other users and eavesdroppers. This is achieved by establishing a communication session key at the end of the authentication process. This session key is used to secure the communication between the end parties. We will be using symmetric key based cryptosystems for securing communications between mobile stations. This choice is due to less computational time required for performing symmetric key based computations compared to the public key ones.

- *User Identity Confidentiality* : In practice, there may be several reasons why the users might wish to keep their identities secret from other users. There can be different degrees of anonymity. For instance, a mobile user A may wish to be known only to the network authorities (e.g. the Authentication Servers) and to the other communicating party B, while remaining anonymous to other network users. We will refer to this form of anonymity as the first degree anonymity. At a higher level, a user A may wish in addition to remain anonymous even with respect to the visiting domain's Authentication Server. We will refer to this as the second degree anonymity. In principle, there is no need for the visiting authority to know the real identity of a user from another domain. What it needs is only a proof of the solvency of the entity accessing the service and enough information to bill the user's home authority correctly.

  We address this issue of anonymity by introducing the notion of a subliminal identity (a form of alias), written as ID_s. Each user is issued a subliminal identity by the home domain H at the time of initial registration. The subliminal ID is composed of a number (e.g. a sequence number) along with a timestamp. This will allow H to perform efficient search of the database when required to locate a specific subliminal ID. Only H knows the mapping between this subliminal ID and the real user ID.

The use of subliminal IDs help to conceal the real user IDs to other network users. A user's subliminal identity can be updated at the end of each authentication session as part of the protocol.

- Non-repudiation of Service: For the service provider, it is desirable that a mobile user subscriber cannot deny the bill for the service he requested. At the same time, the subscriber should not be wrongly charged due to any billing error or security faulty on the network. Theoretically, both goals can be achieved through the use of digital signatures. Given the practical constraint that a mobile unit is not able to perform computationally intensive public key functions, only a limited form of non-repudiation service can be achieved.

- Protocol Design Principles : Domain specific secret information such as a user's long term secret key should not be propagated from the home domain to the foreign visiting domains. Furthermore, it is important to minimize the number of exchanges in the protocol between the home domain and the foreign domain in the setup phase, given that the distance between domains may be large.

4 Security Protocols

4.1 Notation

- $[\,]_K$: Encryption under key K.
- $h(\,)$: Strong one-way hash function.
- $[h(\,)]_K$: Encryption of hashed digest under K.
- PK_X: Public key of X.
- SK_X: Private key of X.
- K_s: Session key shared between A and B.
- H: Home Authentication Server.
- V: Visiting Authentication Server.

4.2 Intra-Domain Authentication and Secure Communication

We now describe the end-to-end authentication protocol between A and B in their home domain (see Figure (2)).

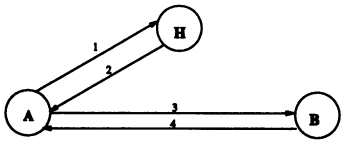

Figure 2: Secure End-to-End Protocol : Intra Domain

4.2.1 Assumptions

- Mobile Station User A (or B):

  Belongs to domain H. Has subliminal identity A_s issued by H and a secret symmetric key K_{AH} (or K_{BH}) shared between A (B) and H.

- Home Server H:

  Has the mapping between the subliminal identity A_s (and B_s) to real identity A (and B). Has public key - private key pair PK_H and SK_H. Has secret symmetric keys K_{AH} and K_{BH}.

4.2.2 Protocol

1: $A \rightarrow H$: $A_s, H, n_A, [A_s, B]_{K_{AH}}, [h(A_s, B, H, n_A)]_{K_{AH}}$

2: $H \rightarrow A$: $H, A_s, n_H, n_A, [B, B_s, K_s]_{K_{AH}}, [A'_s]_{K_{AH}}, [h(H, A_s, B, B_s, A'_s, K_s, n_A)]_{K_{AH}}$, $[A, A_s, K_s]_{K_{BH}}, [h(H, A, A_s, B_s, K_s, n_H)]_{K_{BH}}$

3: $A \rightarrow B$: $A_s, B_s, H, n_H, n'_A, [A, A_s, K_s]_{K_{BH}}, [h(H, A, A_s, B_s, K_s, n_H)]_{K_{BH}}$, $[h(A_s, B_s, H, n_H, n'_A)]_{K_s}$

4: $B \rightarrow A$: $B_s, A_s, n'_A, [h(B_s, A_s, n'_A)]_{K_s}$

In Step 1, mobile computer station A sends a message to its home server H requesting a secure communication with B. In Step 2, H returns a response message including a session key K_s encrypted under the shared key K_{AH} and a new subliminal identity A'_s. The message also includes the K_s encrypted under K_{BV}, which will be passed to B in Step 3. Step 4 completes the authentication and the key establishment process.

Note that the use of the subliminal identity helps to conceal the real identity of the initiator to other system users. In our protocol, we have carefully separated the information which needs to be signed (for integrity and authentication) from that which needs to be encrypted (for confidentiality). It is particularly important to adhere to this principle in the design of protocols; mixing these two aspects leads to lack of clarity in protocol design which is often an important source for protocol flaws. Furthermore this separation is useful when it comes to obtaining export licenses where it is necessary to justify to the authorities the functionality of the various cryptographic interfaces and their use.

4.3 Inter-Domain Protocol and Secure Communication

User A travels to a foreign domain V. When A requests a service to securely communicate with B in V, V needs to ensure that A is a legitimate user from the domain H before providing the service. This authentication process relies on the mutual trust between H and V. Following the authentication process, a secret key to protect communications between A and B can be established. Regarding anonymity, as we mentioned earlier, the real identity of A may need to be hidden from both the eavesdroppers as well as V. There should also be a mechanism for H to issue a new subliminal identity to A. This may be optional.

In the following, we consider a security protocol for the situation where A from H travels to a domain V and requests for secure communication with B in V (see Figure (3)).

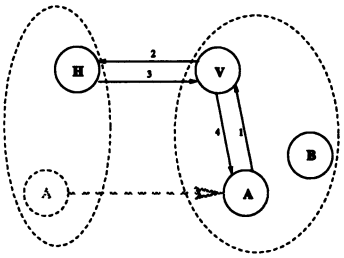

Figure 3: Secure End-to-End Protocol : Inter Domain

4.3.1 Assumptions

- Mobile Station Users A and B:

  Belong to H and V respectively.
  A has subliminal identity A_s and a secret symmetric key K_{AH}, both issued by H.
  B has subliminal identity B_s and a secret symmetric key K_{BV}, both issued by V.

- Home Server H:

  Has the mapping from the subliminal identity to real identity for A.
  Has secret symmetric key K_{AH}.
  Has public key - private key pair PK_H and SK_H as well as the public key of V, PK_V.

- Home Server V:

  Has the mapping from the subliminal identity to real identity for B.
  Has secret symmetric key K_{BV}.
  Has public key - private key pair PK_V and SK_V as well as the public key of H, PK_H.

4.3.2 Protocol

1: $A \rightarrow V$: $A_s, H, n_A, [A_s, B]_{K_{AV}}, Token_{AHV}, [h(A_s, H, n_A)]_{K_{AV}}$,
where $K_{AV} = f(K_{AH}, A_s, V)$ and $Token_{AHV} = [A, H, V, n_A]_{K_{AH}}$

2: $V \rightarrow H$: $V, H, n_V, A_s, Token_{AHV}, [h(V, H, n_V, A_s, Token_{AHV})]_{SK_V}$

3: $H \rightarrow V$: $H, V, n_V, [K_{AV}, A_s]_{PK_V}, [h(H, V, K_{AV}, A_s, n_V)]_{SK_H}, [h(H, n_A)]_{K_{AH}}$

4: $V \rightarrow A$: $V, A_s, n'_V, n_A, [B, B_s, K_s]_{K_{AV}}, [h(V, A_s, B, B_s, K_s, n_A, n'_V)]_{K_{AV}}$,
$[A_s, K_s]_{K_{BV}}, [h(V, A_s, B, n'_V, K_s)]_{K_{BV}}, [h(H, n_A)]_{K_{AH}}$

5: $A \rightarrow B$: $A_s, B_s, V, n'_A, n'_V, [A_s, K_s]_{K_{BV}}, [h(V, A_s, B, n'_V, K_s)]_{K_{BV}}$,
$[A, A_s]_{K_s}, [h(A_s, A, B_s, V, n'_A, n'_V)]_{K_s}$

6: $B \rightarrow A$: $B_s, A_s, n'_A, [h(B_s, A_s, n'_A)]_{K_s}$

In Step 1, A sends V his subliminal identity A_s, communication request $[A_s, B]_{K_{AV}}$, a token $Token_{AHV}$, a nonce n_A, and the signed hash value. $Token_{AHV}$ is encrypted under K_{AH} and it needs to be passed to H by V in Step 2. $Token_{AHV}$ conveys to H that A at present in V wishes to use a service in V. At this stage, V cannot understand the communication request and cannot verify the authenticity of the hash value as it does not have K_{AV}. K_{AV} is generated with a publicly known strong one-way function f. Knowing V and A_s, H is able to calculate K_{AV}, because it shares K_{AH} with A. The mapping of A_s to A is maintained at H.

In Step 2, V sends H the $Token_{AHV}$. The communication is signed by V using its private key (of the public key pair). At the end of this step, H is able to verify that A is making a request to V at the present time.

In Step 3, H sends V the key K_{AV} (encrypted under public key of V), the subliminal identity A_s (encrypted under public key of V). It also sends response information (the freshness component n_A) encrypted under K_{AH} for V to pass to A.

Upon the receipt of H's message, V retrieves K_{AV}, and uses it to verify the hash value that it initially received from A in Step 1. It then generates a session key K_s for use between A_s and B. The K_s is encrypted under K_{AV} for A, and is also encrypted under K_{BV} for B. All of this is then sent to A in Step 4. The information $[h(H, n_A)]_{K_{AH}}$ that V received from H is also passed to A.

In Step 5, A passes to B the session key that it received from V. Finally Step 6 completes the authentication and the key establishment process.

As an option, H may issue a new subliminal identity A'_s for A as part of this protocol. This can be done by including the following information in Step 3: $[A'_s]_{K_{AH}}$, $[h(H, A'_s, n_A)]_{K_{AH}}$ (instead of $[h(H, n_A)]_{K_{AH}}$). This portion of the message will then be passed by V to A in Step 4.

5 Discussion

It is worth discussing the following characteristics of the above protocol.

- The real identity of the mobile station user A is not revealed to system users other than B. That is, the first degree anonymity is achieved. Furthermore, the real

identity of A is not revealed to V. Similarly the identity of B is not revealed to H. Hence the second degree anonymity is also achieved. A useful discussion of anonymity can be seen in Ref. (Asokan, 94).

- The protocol provides an option for changing the subliminal identity during every session if required. On the other hand, for the period of time that A is going to be within the domain V and using its services, it may be sufficient to keep the same subliminal identity. In this case, V and A can share K_{AV} for this period of time resulting in the optimization of subsequent protocol exchanges.

- It is possible to include the nonce n_A as part of the calculation of K_{AV}. In this case, K_{AV} can be changed every request even if the A_s parameter remains constant for a period of time.

- Given that K_{AV} can only be calculated by H and A, and that H is trusted by both V and A not to generate $[h(A_s, H, n_A)]_{K_{AV}}$ illegally, the possession of communication request encrypted under K_{AV} by V indicates that it has been generated and sent by A sometime earlier. At the same time, given that A trusts H and that V (or any one else) cannot generate the request under K_{AV}, one can ensure that A is not charged wrongly.

- Session key K_s that is used for communication is changed every request. Hence even if one K_s is compromised, future communications can be protected.

- There are several options as to who generates the key K_s. In the protocol proposed, we have assumed that V generates K_s and distributes it to A and B. This seems natural when both A and B are in V's domain. When A and B are in two different domains, either H or V can generate the session key K_s.

- There are various options for distributing the session key K_s to B. We have chosen the option whereby V passes K_s to B via A. Other alternatives include V passing the session key directly to B (which may lead to timing problems) or asking B to pass the session key to A.

- At the end of Step 4, A has received from V the information $[h(H, n_A)]_{K_{AH}}$ sent by H in Step 3. This helps A to believe that its request has been passed to H and H has provided the right information to V.

- Note the asymmetricity in the use of A_s and B_s in the protocol exchanges. This is based on the principle that H only knows the true identity of A (and not B), and V only knows the true identity of B (and not A).

- Public key system has been only used between V and H and not between H and A or V and A. This reduces the complexity of the computations.

REFERENCES:

Asokan, N. (1994), Anonymity in a mobile computing environment, In *Proceedings of*

1994 IEEE Workshop on Mibile Computing Systems and Applications.

Cox, D. C. (1990), *IEEE Communications Magazine* **27**.

Molva, R., Samfat, D., and Tsudik, G. (1994), *IEEE Network* , 26–34.

Varadharajian, V. (1995), Security for Personal Mobile Networked Computing, In *Proceedings of the International Conference on Mibile and personal Communications Systems.*

Varadharajian, V. and Mu, Y. (1996), Design of Security Protocols for Mobile Systems : Symmetric Key Approach, In *Proceedings of the rth International Conference on Wireless Communications,* (to appear).