Wireless Client Server Application Model Using Limited Key Generation Technique

Rohit Singh
Monash University, Australia

Dhilak Damodaran
Monash University, Australia

Phu Dung Le
Monash University, Australia

INTRODUCTION

The introduction of personal digital assistants (PDAs) and laptops has brought in mobility for carrying out computing jobs (Pasquale, Hung, Newhouse, Steinberg, & Ramabhadran, 2002; Varshney & Vetter, 2000). Wireless networks in working areas cater the need for installation flexibility, reduced cost-of-ownership, mobility and scalability. Mobile computing is distinguished from classical, fixed-connection computing due to the mobility of nomadic users and their devices (Jing, Helal, & Elmagarmid, 1999) and mobile environment is defined as low bandwidth and high latency networks with devices supporting limited input methods and containing low power processors, small display size and short battery life (Buszko, Lee, & Helal, 2001). Mobile working environments attract the users, employees and students, but presents hardships to the security programmer because the settings and the environment of mobile devices vary significantly from that of wired devices.

The ease of network access should be combined with reliable security services. Wireless networks are exposed to the security compromises because it provides hacker easy access to transport media. An attacker can sniff the packets by setting up equipment monitoring at 2.4GHz frequencies and capable of interpreting the packets of 802.11 standard (Borisov, Goldberg, & Wagner, 2001; IEEE Standard 802.11b, 1999; Josang & Sanderud, 2003). This unauthorized access to the network is a matter of great concern for any network security administrator. Cryptography, that is encryption of the data, is one of the best ways to provide security to wireless communication. Even the strongest of the encryption procedures can become vulnerable to possible attacks when the keys of the parties get compromised. Thus the lack of security is predominantly due to poor management of keys rather than the weakness in the encryption algorithm (Josang & Sanderud, 2003).

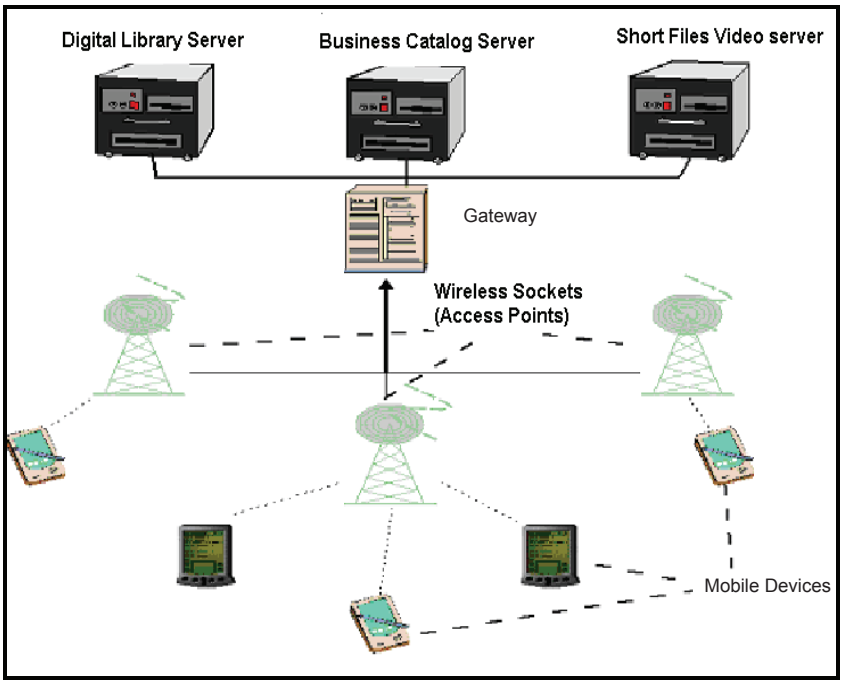
In this article we implement a client server model using limited-used key generation scheme (Kungpisdan, Le, & Srinivasan, 2004) to generate a set of session keys that are never transmitted, which means that there is no chance for the attacker to sniff the packets and retrieve keys while they are being transmitted. These session keys are used for encrypting and hashing the data to be transmitted from mobile client device to the servers in wired network and vice versa. The updating of the session keys used in this technique does not rely on any long-term shared key, instead the process is based upon the last session key used. This technique of elevating the frequency of the key update to the next possible level makes the system much more secure than the other present techniques. In addition to providing better security, this technique also enhances the performance of a limited resource device by avoiding the repeated generation of keys on it.

The rest of the article is organized as follows. The second section gives an overview of the communication between mobile devices and the various servers running in the wired network. The third section describes the proposed technique. The fourth section discusses the technique in applied state. Next, the fifth section discusses about other key management and security issues of the technique. The last section concludes the article.

CLIENT SERVER MODEL

The client server model in a wireless environment is depicted in Figure 1. Mobile clients in wireless networks first connect to an access point, which is connected with wired media to the main network infrastructure. After a successful connection with the access point, mobile clients can start communicating with the gateway and servers that are present within the main network. The model described in this article proposes to set up a gateway program which authenticates every mobile client before it connects to any server inside the main network. The authentication is carried on the basis of the technique discussed in the fourth section. The gateway program can be executed at the gateway server of organization.

Figure 1. Remote access model



The course of action that is carried out in the proposed protocol is as follows:

- **C → G:** Server Connection (Request), Command Execution (Request)
- **G → S:** Command-Execution (Request)
- **S → G:** Command-Execution (Response)
- **G → C:** Server Connection (Response), Command-Execution (Response)

PROPOSED TECHNIQUE

Notations

- *{C, G, S}*: the set of clients, gateway and server, respectively.
- $\{K_A, K_A^{-1}\}$: the set of public/ private key for party A.
- $\{ID_C, ID_S, ID_G\}$: the set of identities of client, the server and the gateway respectively.
- $ID_G Req$: request for ID_G
- *CI*: Command execution information.
- *CRes*: Command response
- $\{M\}_X$: the message M symmetrically encrypted with the shared key *X*.
- $\{M\}_{Kx}$: the message M encrypted with the public key of the party *X*.
- $\{M\}_{Kx}^{-1}$: the message M signed with the private key of the party *X*.
- *h (M)*: the one-way hash function (FIPS, 1995) of the message *M*.
- *MAC (M, K)*: the message authentication code (*MAC)* of the message *M* with the key *K*.

Initial Assumption and Settings

Initial assumptions and settings for the proposed technique are as follows:

1. Client is considered to be a person with the wireless device and has access to the organization's network.
2. Client's employment record (CER), containing employee code and other information about the client, is the long-time shared secret between the server and Client. CER is assumed to be a key that never expires.
3. The distributed key DK is another shared key between client and server. This key is distributed by performing authenticated key exchange (AKE) (Boyd & Park, 1998; Horn & Preneel, 1998; Kungpisdan, Le, & Srinivasan, 2003; Toh, Kungpisdan, & Le, 2004; Wong & Chan, 2001; Zhu, Wong, Chan, & Ye, 2002) protocol between client and server.