블루투스 모바일 폰을 위한 보안인증 시스템

Security and Authentication System for Bluetooth Mobile Phone

발라칸난 S.P*, 이문호*, 카틱B**
Balakannan.S.P[1], Moon Ho Lee[1], Karthik.B[2]

Abstract - Authentication is a mechanism to establish proof of identities, the authentication process ensure that who a particular user is. Nowadays PC and laptop user authentication systems are always done once a hold until it's explicitly revoked by the user, or asking the user to frequently reestablish his identity which encouraging him to disable authentication. Zero-Interaction Authentication (ZIA) provides solution to this problem. In ZIA, a user wears a small authentication token that communicates with a laptop over a short-range, wireless link. ZIA combine authentication with a file encryption. Here we proposed a Laptop-user Authentication Based Mobile phone (LABM). In our model of authentication, a user uses his Bluetooth-enabled mobile phone, which work as an authentication token that provides the authentication for laptop over a Bluetooth wireless link, in the concept of transient authentication with our combining it with encryption file system. The user authenticate to the mobile phone infrequently. In turn, the mobile phone continuously authenticates to the laptop by means of the short-range, wireless link.

Key words : Mobile Computing, Authentication, Bluetooth

1. Introduction

In recent years, many people use their office PC or home PC for their work and store the sensitive information, at the same time mobile computing has enjoyed a tremendous rise in popularity. As laptops proliferate, theft has become an ever more critical security issue. Within the much broader arena of IT security, there are five classes of technology that are most relevant to laptops. These are: User authentication, Physical locking devices, Encryption, Monitoring and tracing software and Alarms [1]. The key aspect of cryptography and computer security is authentication [2]. Authenticate help establish trust by identifying who a particular user is. Authentication ensures that the claimant is really what he/she clam to be. User authentication is a required component of all security systems.

Persistent and Authentication-Users authenticate infrequently to devices. User authentication holds until it is explicitly revoked. Currently, most of the systems use this technique [3]. Should a device fall into the wrong hands, the imposter has the full rights of the legitimate user while authentication holds. Persistent authentication creates tension between protection and usability. To maximize protection, a device must constantly reauthenticate its user. To be usable, authentication must be long-lived. If someone steals your laptop while you are logged in, the have full access to your data. Such persistent authentication is inappropriate for mobile computers. This tension of persistent authentication resolved with a new model, called transient authentication [4]. In this model, user wears a small token, equipped with a short-range wireless link and modest computational resources. This token is able to authenticate constantly on the user's behalf. Transient authentication shifts the problem of authentication to the token.

We implement an authentication model for laptop devices that uses cell phones as authentication token. In this model a user uses his mobile phone which works as an authentication token, that provide the authentication forlaptop over a short-range wireless link as shown in Fig 1.

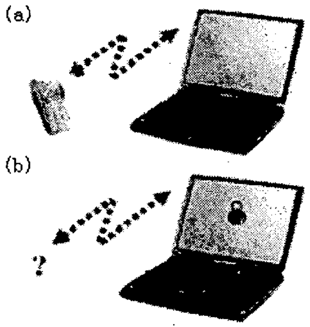

Fig 1: (a) Unsecured Mode (User Present)
(b) Secure Mode (User Absent)

2. Design and Implementation

The Authentication system design consists of three parts:

- ■ Laptop-Cell phone authentication system
- ■ User authentication system
- ■ Communication module

2.1 Laptop-Cell phone Authentication System

The security applications of the algorithm perform four functions: Mutual authentication, User notification, Create session key, Disconnection and reconnection. The over all processes of authentication system illustrated in Fig.2.

The mutual authentication is the first step in the authentication system. In this step the system perform a challenge-response function between the laptop and mobile phone in order to authenticate each other based on public key system [5]. The mobile phone and Laptop has predefined key pair.

After performing the mutual authentication between user and his/her cell phone the cell phone notify user

저자 소개

* 발라칸난 S.P : Chonbuk National University, Jeonju 561 756. South Korea. {balakannansp@gmail.com}

* 이 문 호 : Chonbuk National University, Jeonju 561 756. South Korea. {moonho@chonbuk.ac.kr}

** 카 틱 B : Programmer, Sri Ramakrishna Engineering College, Coimbatore, India. {karthikbellan@yahoo.com}

about the connection that has been established and ask for user agreement. Whenever users agree for the connection, the system does not ask him/her again and cell phone takes all responsibility for authentication system.

Session key is used to encrypt all laptop-mobile phone communication. Once session key is established, all information that transfers over the wireless link will not be in clear text format; instead it will be encrypted and authenticated using a session key. The creation of symmetric session key is done based on Diffie-Hellman Key Exchange Agreement/ Algorithm [6].

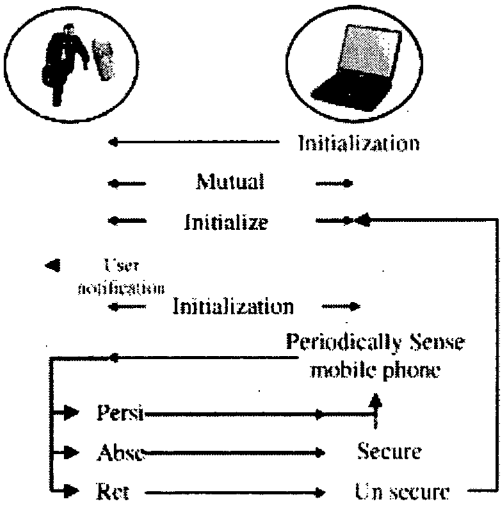

Fig 2 : Laptop-Cell Phone authentication System

The system periodically sense mobile phone to ensure that the user is still present or not. When the mobile phone is out of range, the laptop will take step to secure it self. There are two reasons why laptop not receives a response from the mobile phone. 1. The mobile phone and the user are truly being away, or 2. The link may have dropped the packet. For the latter the system uses expectedround trip time between laptop and mobile phone, because this is a single, uncontested network hop. Laptop retries request if responses are not received within twice the expected round trip time.

2.2 User Authentication System

Authentication between user andhis/her mobile phone both are infrequent and persistent, when the mobile phone asks for user authentication. This authentication holds until it explicitly revoked. Normally the cell phones use a PIN code for user authentication.

3. Communication Module

The communication module is implanted through UDP. Each datagram data field is simply the text inputted, after passing it through the encryption function as described earlier. The module opens up a Bluetooth port in both laptop and mobile phone for receiving communications. Once it receives a packet, it attempts to decrypt that packet based on the session key currently created, and uses the results according to current function.

4. Devices Connectivity

The communication module establishes a typical single slave Bluetooth pico net scenario (point-to-point), where the mobile phone acts as a master while the laptop acts as slave. The communication uses the Bluetooth data channel, where the data can be exchange at a rate of approximately 720 Kbps using point-to-point encrypted connection. The range is approximately 10m.

4.1 Link Manager Protocol (LMP)

The LMP is used for link setup and control process in which two devices transfer handshaking information. Logical Link Control and Adaptation Protocol (LLCAP) provide connection oriented and connectionless data services to upper layer protocols with protocol multiplexing capacity. LLCAP permits higher-level protocols and applications to transmit and receive LLCAP data packets up to 64 Kb in length, since it supports Internet Protocol datagram's.

4.2 Service Discovery Protocol (SDP)

Service Discovery Protocol is part of LMP. It provides a means for applications to discover which devices/services are available and to determine the characteristics of those available devices/services, a necessary first step before a connection between two devices can occur, SDP uses a request/response model where each transaction consists of one request Protocol Data Unit (PDU) and one response PDU.

4.3 Connection Establishment at Laptop Side

The laptopacts as client side in the pico nets, its communication consists of initializing the Bluetooth stack, discovering mobile phone that is in proximity, open,close and initiate connections, and perform security application Input/Output (I/O) messages. Bluetooth initialization typically retails setting the device's name, security settings, and/or turning the Bluetooth radio on/off. These aforementioned steps are done via what is referred to as the Bluetooth Control Center (BCC), which typically are a set of control panels that serves as the central authority for local Bluetooth device settings. Creating Bluetooth connections aredone using the LLCAP of the Bluetooth protocol stack. LLCAP does a simple NSLOOKUP and gets the address of the mobile phone and tries to establish a logical connection with the LLCAP of the master through the Host Controller Interface layer below. After creating connection the application performs the security function I/O messages that describe.

4.4 Connection Establishment at Mobile phone Side

The mobile phone acts as server side in the pico nets, it performs same client function except that instead of initializing and opening connection it creates a server connection using the LLCAP and waiting for connections, accept and open connections, and perform security application I/O messages. Before creating the connection the application the application get the local device, and make it to discoverable however the client (laptop) can establish a connection and start to perform security I/O messages and mange connection according to its results.

5. Implementation

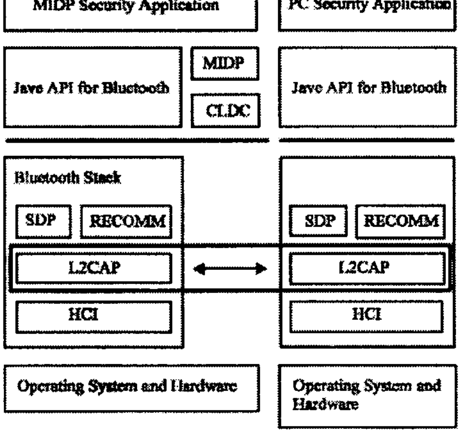

Fig.3. Using Java APIs in Communication Mobile.

The model is implemented in application layer it consists of a client runs on the user's laptop and server runs on the user's mobile phone, communicating via Bluetooth wireless secured channel. All programs are written using pure Java and Java APIs for Bluetooth. Fig.3 illustrates Java APIs with communicating layers. We choose Java over other programming languages because of the availability of the numerous functions in the Java API, which allowed us to focus more on the abstract ideas rather than low-level programming.

6. Result

System declares user absent after three tires to connect to mobile phone without response. The time required by laptop program to declare user absent and secure laptop by run semi screen server threaded program. Laptop continues sense the return of the mobile phone and hence the user to stop security program and reconnect user.

7. Comparison with Existing Related Work

Zero Interaction Authentications (ZIA) system that provide encrypted filling services that defend against physical attack while imposing negligible usability and performance burdens on a trusted user is ZIA. The authentication based ZIA is depend on providing decryption services for encryption key used in laptop and stored on it in encryption format. The user with ZIA must be encryption file system, and the user authentication part is not separated from encryption part.

Microsoft Windows 2000 provides user reauthentication feature in case of sensing absent of user according to tracing keyboard, and mouse movement rather than real departure of the authorized user. The reauthenticationfeature depends on screen saver to get access where the user must reapply his/her identity. The user may disable the screen saver after finding it intrusive. Biometric authentication still has some problems like false-negative rate, and for transient authentication it also needs reauthentication by user.

8. Feature Work

The cell phone application could include more additional security functions, if the laptop uses a data encryption technique to encrypt data on its hard disk that can deal with the transient authentication mechanism like ZIA [7], the mobile phone can provide a decryption service to laptop data encryption key, which stored in laptop in encrypted format using a predefined decryption key stored in mobile phone. Also the mobile phone can provide storing and management services for key used in laptop encryption instead of storing the key inside laptop itself. The cell phone with Bluetooth technology and java API's for Bluetooth could be uses for in many useful authentication systems.

9. Acknowledgment

This work was supported by Minister of Information and Communication (MIC) supervised by IIFA and ITRC supervised by IITA, ITSOC and International Cooperative Research Program of the Ministry of Science and Technology, KOTEF and 2nd stage BK21, Chonbuk National University, South Korea.

10. References

[1] Laptop Computer Security, White Paper. Caveo Technology, March 2003.

[2] Burrows.M., M.Abadi, and R.Needham, 1990. Logic of authentication. ACM Transaction on Computer Systems, 8:18-36.

[3] Corner.M.D and B.D Nobel, 2002. Zero interaction authentication. In proceeding of the ACM International Communication. Atlanta, Georgia, USA.

[4] Nobel B.D . and M.D. Corner, 2002. The case for transient authentication. In Proceedings of 10th ACM SIGOPS European Workshop, SintEmillion, France.

[5] Kahate.A.2003. Cryptography and Network Security, 1st Edn, Tata McGraw-Hill Company.

[6] Daemen.J., and V. Rijimen, 1999. AES proposal: Rijndael, Advanced Encryption Standard Submission, 2nd Version.

[7] Kammann.J., T.Strang K.Wendlandt, 2001.Mobile services over short-range communication. Workshop commercial Radio Sensors and communication Techniques