Journal of Computer Science 1 (2):200-203, 2005
ISSN 1549-3636

Authentication Model Based Bluetooth-enabled Mobile Phone

Rania Abdelhameed, Sabira Khatun, Borhanuddin Mohd Ali and Abdul Rahman Ramli
Department of Computer and Communications Systems Engineering, Universiti Putra Malaysia
43400, Kuala Lampur, Malaysia

Abstract: Authentication is a mechanism to establish proof of identities, the authentication process ensure that who a particular user is. Current PC, laptop user authentication systems are always done once and hold until it 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 out 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: Authentication, Mobile Computing, Bluetooth

INTRODUCTION

In recent years, many people use their office 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, 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 Transient Authentication: Persistent 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, they 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, a 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 phone as authentication token.

Laptop-Cell Phone Authentication System Principles: In this model of authentication, a user uses his mobile phone which works as an authentication token, that provide the authentication for laptop over a short-range wireless link as shown in Fig. 1. The user authenticate to the token infrequently. In turn, the mobile phone continuously authenticates to the laptop by means of the short-range, wireless link [5].

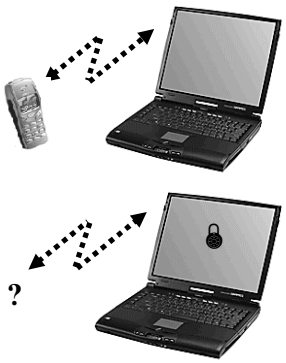

Fig. 1: (a) Unsecure Mode (User Present), (b) Secure Mode (User Absent)

DESIGN AND IMPLEMENTATION

Authentication System Design: The system design consists of three parts:

* Laptop-Cell phone authentication system.
* User authentication system
* Communication module

Laptop-Cell phone Authentication System: The security applications of the authentication 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.

Mutual Authentication: 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 [6]. The mobile phone and has predefined key pair.

User Notification: After performing the mutual authentication between user and his/her cell phone the cell phone notify user about the connection that has been established and ask for user agreement. Whenever user agree for the connection the system dose not ask him/her again and cell phone take all responsibility for authentication system.

Session Key Creation: 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 [7].

The system uses the U.S. government standard 128- Bit Advanced Encryption Standard (AES) [8] to encrypt all laptop–mobile phone communication, we chose this method because it is the current Advanced Encryption Standard (AES) chosen by the National Institute of Standards and Technology (NIST), and it is fast enough to run efficiently with limited memory resources and processing time.

Disconnection and Reconnection: The system periodically sense mobile phone to ensure that the user is still present, when the mobile phone is out of the range the laptop take step to secure it self. There are two reason why laptop not receive a response from the mobile phone, the mobile phone and the user are truly be away, or the link may have dropped the packet. For the latter the system uses expected round trip time between laptop and mobile phone, because this is a single, uncontested network hop, this time is relatively stable. Laptop retries request if responses are not received within twice the expected round trip time.

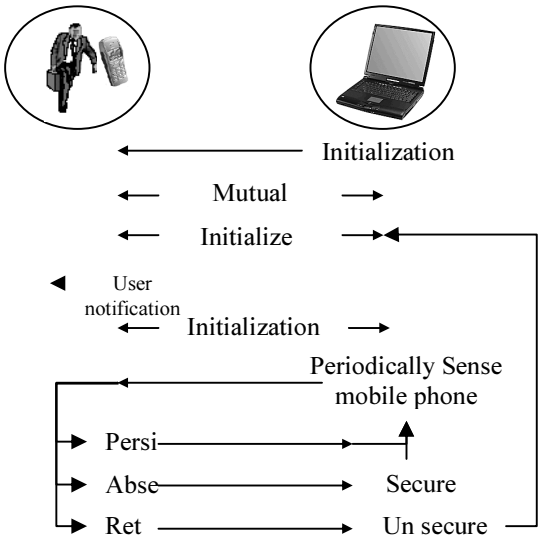

Fig. 2: Laptop-cell Phone-authentication System

User Authentication System: Authentication between user and his/her mobile phone both 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.

Communication Module: The communication module is implemented through UDP. Each datagram is 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.

Devices Connectivity: The communication module establishes a typical single slave Bluetooth piconet scenario (point-to-point) [9], where the mobile phone acts as a master while the laptop acts as slave. The communication uses the Bluetooth data channel, where data can be exchange at a rate of approximately 720 Kbps using point-to-point encrypted connection. The range is approximately 10 m.

Connection at Physical and Data Link Layers: The core Bluetooth protocols of data link and physical layer uses in the connection model is:

Baseband: Baseband and Link Protocol enable the physical RF connection between devices.

Link Manager Protocol (LMP): The Link Manager Protocol is used for link setup and control process in which two devices transfer handshaking information. The signals are interpreted and filtered out by the Link Manager on the receiving side and are not propagated to higher layers. Logical Link Control and Adaptation Protocol (L2CAP): L2CAP provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capacity,

segmentation and reassembly operation, and group abstraction. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 Kilobytes in length, since it supports Internet Protocol (IP) datagrams.

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.

Connection Establishment at Laptop Side: The laptop acts as client side in the piconets, its communication consists of initializing the Bluetooth stack, discovering mobile phone that is in proximity, open and close and initiate connections, and perform security application I/O messages. Bluetooth initialization typically entails 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. Before creating the connection the application retrieve local device information that uses for creating connection. Creating Bluetooth connections is done using the Logical Link Control and Adaptation Layer (L2CAP) of the Bluetooth protocol stack. L2CAP does a simple NSLOOKUP and gets the address of the mobile phone (server or master) and tries to establish a logical connection with the L2CAP of the master (mobile phone) through the Host Controller Interface (HCI) layer below.After creating connection the application performs the security function I/O messages that described in section 4.1.

Connection Establishment at Mobile phone Side: The mobile phone acts as server side in the piconets, it performs same client function except that instead of initializing and opening connection it creates a server connection using the L2CAP and waiting for connections, accept and open connections, and perform security application I/O messages. Before creating the connection the application get the local device, and make it to discoverable however the client (laptop) can establish a connection to it. When mobile phone receives a L2CAP connection request it accept and open connection and start to perform security I/O messages and mange connection according to its results.

Implementation: 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 [10].

All programs are written using pure Java technology: Java 2 Standard Edition (J2SE), Java 2 Micro Edition (J2ME)/Connected Limited Device Configuration (CLDC)/Mobile Information Device Profile (MIDP) and Java APIs for Bluetooth (JSR-82). Figure 3 illustrates Java APIs with communicating layers.

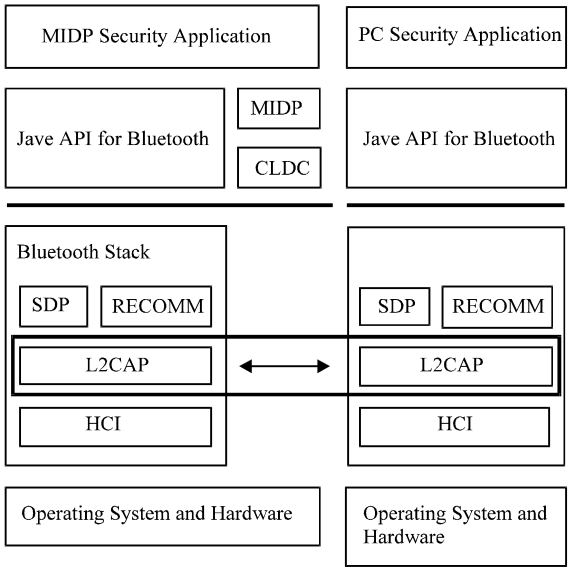

Fig. 3: Using Java APIs in Communication Module

We chose 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.

RESULTS

System declares user absent after three tries to connect to mobile phone without response. The line in Figure 4 show the time required by laptop program to declare user absent and secure laptop by run semi screen sever threaded program.Laptop continues sense the return of the mobile phone and hence the user to stop security program and reconnect user. The line in Figure 5 show the time required by laptop program to reconnect user and stop security thread.

Comparison with Existing Related Work: Zero Interaction Authentication (ZIA), The first system that provide encrypted filing 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

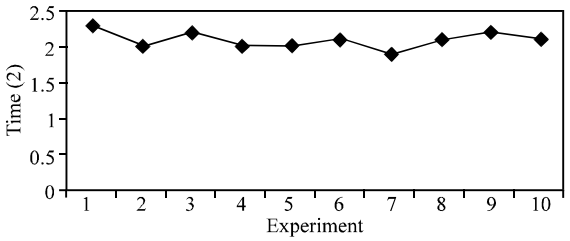

Fig. 4: Time Required for User Disconnection

Table 1: Comparison with ZIA System

	ZIA	LABM
Functionality	Authentication and Encryption File System	Authentication
Wireless Link	IEEE 802.11 b Distance: 30-00 m Speed: 11 Mbps	Bluetooth Distance: 10 m max Speed: 720 Kbps
Token	IBM Linux watch	Mobile phone
Disconnection Time	Depend on size of cached file pages	Approximately fixed Longer Shorter (no file system encryption required)
Reconnection Time	Depend on cached key and size of cached file pages	Approximately fixed
Security	More secure	Less secure
Complexity	More complex	Less complex
Weaknesses	Loss of token. Requires key management	Loss of mobile phone
Source Code	Written in C++	Written in pure Java

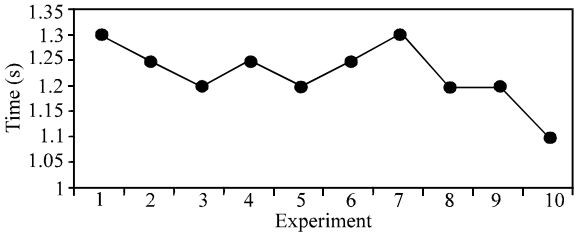

Fig. 5: Time Required for User Reconnection

must use encryption file system, the user authentication part is not separated from encryption part. Table 1 shows comparison between LABM and ZIA system. 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 reauthenticate feature depends on screen saver to get access where the user must resupply 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.

Future 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 [9], the mobile phone can provide a decryption service to laptop data encryption key, which stored in laptop in encrypted format using a pre defined 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 APIs for Bluetooth could be uses for in many useful authentication systems.

ACKNOWLEDGMENT

The first author would like to acknowledge her fellowship for graduate study (M.Sc. in Computer System Engineering) from Third World Organization for Women in Science (TWOWS) and research partially support by IRPA Grant No. 04-02-04-0186EA001.

REFERENCES

1. Laptop Computer Security. White paper, Caveo Technology, March 2003.
2. Burrows, M., M. Abadi, and R. Needham, 1990. A logic of authentication. ACM Transaction on Computer Systems, 8: 18-36.
3. Corner, M.D. and B.D. Noble, 2002. Zero interaction authentication. In Proceeding of the ACM International Conference on Mobile Computing and Communications (MOBICOM'02), Atlanta, Georgia, USA.
4. Noble, B.D. and M.D. Corner, 2002. The case for transient authentication. In Proceeding of 10th ACM SIGOPS European Workshop, Saint-Emillion, France.
5. Hu, Y., A. Perrig, and D.B. Johnson, 2002. Wormhole detection in wireless ad hoc networks. Technical Report, Department of Computer Science, Rice University.
6. Kahate, A., 2003. Cryptography and Network Security. 1st Edn. Tata McGraw-Hill Company, India.
7. Daemen, J., and V. Rijmen, 1999. AES proposal: Rijndael. Advanced Encryption Standard Submission. 2nd Version.
8. Chang, J.K.W., 2003. An interaction of bluetooth technology for zero interaction authentication. Honours Project, School of Computer Science, Carleton University.
9. Kammann, J., T. Strang and K. Wendlandt, 2001. Mobile services over short range communication. Workshop Commercial Radio Sensors and Communication Techniques, TU Inz, Austria.
10. Angermann, M., P. Robertson and A. Steingaß, 1991. Integrationof navigation and communication services for personal travel assistance using an java and jini based architecture. In Proc. GNSS1999, Genua, Italy.