Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 5 (2): 215-219, 2005
ISSN 1812-5654

Application of Cell-phonein Laptop Security

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

Abstract: Authentication is a mechanism help 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. 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 short-range wireless link, in the concept of transient authentication. 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[1], monitoring and tracing software, alarms. The key aspect of cryptography and computer security is authentication[2]. Authentication help establish trust by identifying who a particular user is. Authentication ensure 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: Users authenticate infrequently to devices. User authentication holds until it is explicitly revoked, though some systems further limit its duration to hours or days-it is persistent. Currently, systems assume that the user typing now is the same person who supplied a password days ago. Authentication between people and their devices is both infrequent and persistent[3]. Should a device fall into the wrong hands, the imposter has the full rights of the legitimate user while authentication holds.

One way to limit the vulnerabilities of persistent authentication is to limit its duration. This increases the user's burden, encouraging him to disable security entirely. 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.

Persistent authentication has been acceptable for personal computing because PCS have relatively strong physical security. However, mobile devices are easily carried and therefore easily lost or stolen; 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 of authentication, 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. It also acts as a proximity cue to applications and services; if the token does not respond to an authentication request, the device can take steps to secure itself. Transient authentication shifts the problem of authentication to the token.

We implement an authentication model for laptop devices that use cell phone as authentication token.

PC and laptop marketing: Despite the slowdown in the overall personal computer (PC) market, growth in laptop computers continues. According to Gartner, worldwide laptop sales grew 11.6% in 2002, compared with only 2.7% growth in PCS overall[3]. Worldwide growth for PCS is projected to return to high single digit levels in 2003. The

Corresponding Author: Rania Abdelhameed, Department of Computer and Communications Engineering,
Universiti Putra Malaysia 43400, Kuala Lampur, Malaysia E-mail: eng_rani@hotmail.com

(a) (b)

Fig. 1: (a) Un secure mode (user present), (b) Secure mode (user absent)

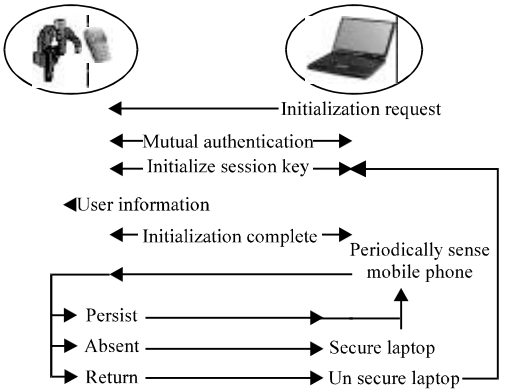

Fig. 2: Laptop-cell phone-authentication system

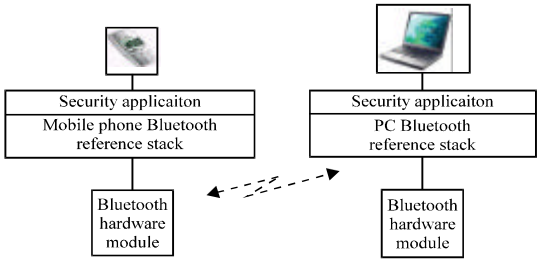

Fig. 3: Communication module

laptop--increasingly the computer of choice for both business and consumer buyers--will likely to continue growth at double-digit levels.

Laptop-cell phone authentication system principles: In this model of authentication, a user uses his mobile phone which work 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 secured short-range, wireless link[5].

Authentication system design

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 authentication: 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.

Session key creation: Session key is uses 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].

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.

Encryption and decryption process: The system uses the U.S. government standard 128-bit advanced encryption standard[7] to encrypt all laptop-mobile phone communication, we chose this method because it is the current advanced encryption standard chosen by the National Institute of Standards and Technology and it is fast enough to run efficiently with limited memory resources and processing time. The over all processes of authentication system illustrated in Fig. 2.

Communication module: The communication module is implemented through UDP. Each datagram in data field is simply the text inputted, after passing it through the encryption function as described earlier. The module establishes a typical single slave Bluetooth piconet scenario (point-to-point)[8], it opens up a Bluetooth port in both laptop and mobile phone for receiving communications as shown in Fig. 3.

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.

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.

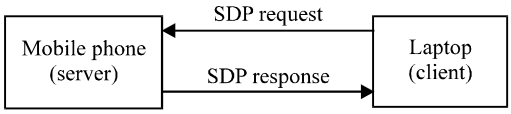

Fig. 4: SDP request/response model

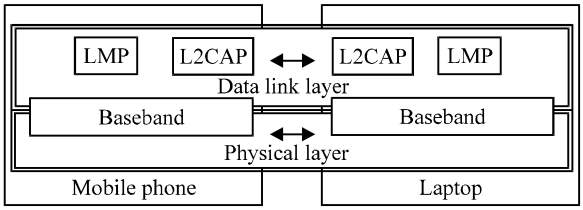

Fig. 5: Connection at data link and physical layers

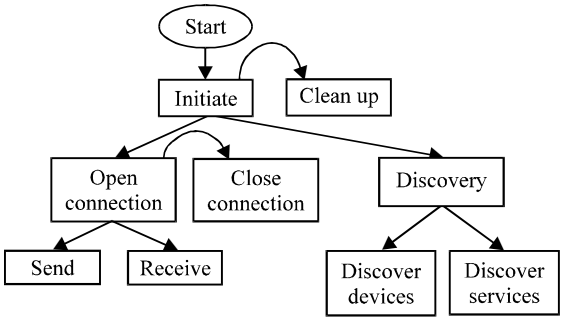

Fig. 6: Laptop (client side) connection functions

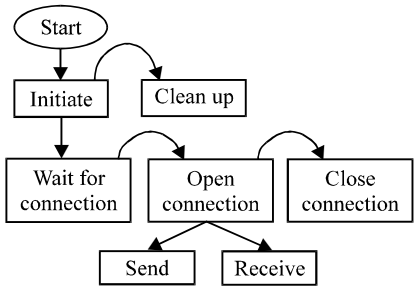

Fig. 7: Mobile phone (server side) connection functions

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. Link manager messages have higher priorities that user data. This means that if the link manager needs to send a message, it shall not be delayed by the L2CAP traffic, although it can be delayed by many retransmissions of individual baseband packets.

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 KB 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 as shown in Fig. 4.

Figure 5 show the connection of devices at both data link and physical layers.

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 as shown in Fig. 6.

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 was described previously.

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 as shown in Fig. 7.

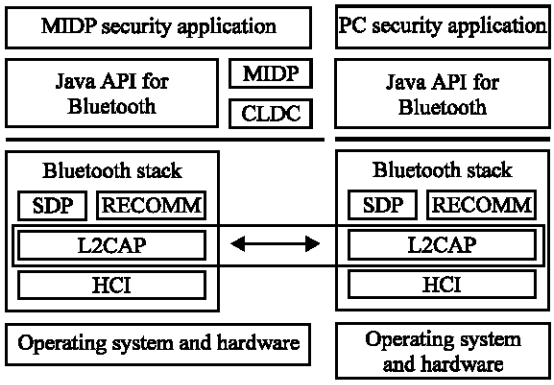

Fig. 8: Using of Java APIs in communication module

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 receive 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[9].

Laptop system: The laptop client part written using Java 2 standard edition (J2SE) and java APIs for Bluetooth. This is a java technology that has been customized specially for the platform of a desktop computers, workstations and laptops where java API for Bluetooth provides a common API for Bluetooth development[10].

Mobile phone system: The mobile phone server part written using java 2 micro edition (J2ME)/connected limited device configuration (CLDC)/mobile information device profile (MIDP) and java APIs for Bluetooth (JSR-82). This is a java technology that has been customized specially for the platform of a desktop computers, workstations and laptops. Mobile phone must laptop request.

Figure 8 illustrates java APIs with communicating layers.

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. Figure 9

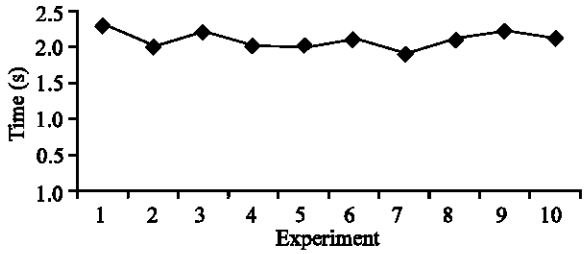

Fig. 9: Time required for user disconnection

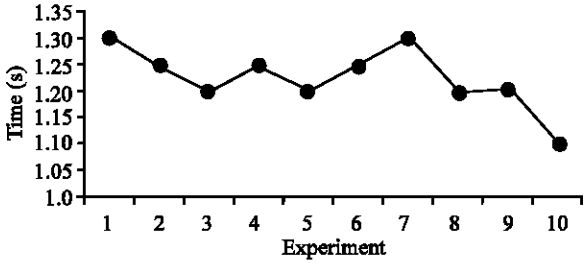

Fig. 10: Time required for user reconnection

shows 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. Figure 10 shows the time required by laptop program to reconnect user and stop security thread.

System security: There are two concepts in system security:

- User's mobile phone cannot provide authentication services to other user's laptops.
- Mobile phone cannot send authentication messages over wireless link in clear text form.

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 research funding from Third World Organization for Women in Science (TWOWS) for funding her graduate (M.Sc.).

REFERENCES

1. Blaze, M., 1993. A cryptographic file system for UNIX. In Proceedings of the 1st ACM Conf. Computer and Communications Security, Fairfax, VA., pp: 9-16.
2. Burrows, M., M. Abadi and R. Needham, 1990. A Logic of Authentication, ACM Transaction on Computer Systems, USA., 8: 18-36.
3. Corner, M.D. and B.D. Noble, 2002. Zero interaction authentication. In Proc. ACM Intl. Conf. Mobile Computing and Comm. (MOBICOM'02), Atlanta, Georgia, USA.
4. Noble, B.D. and M.D. Corner, 2002. The case for transient authentication. In Proc. 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, 1999. Integration of navigation and communication services for personal travel assistance using an java and jini based architecture. In Proc. GNSS1999, Genua, Italy.