Remote Access And Networked Appliance Control Using Biometrics Features

Mahfuzur Rahman, Member, IEEE and Prabir Bhattacharya, Fellow, IEEE

Abstract — *With the advent of home networks and the proliferation of broadband connectivity to homes, there is an increasing demand for a secure end-to-end mechanism to remotely access home networks and control home appliance from remote sites on the other side of the Internet. In this paper we propose an architecture for secure access to home or an organization's networks and control of networked appliances inside a home or within an organization from a remote location. We use biometrics features and a one-time password mechanism on top of secure socket layer (SSL) for authentication. We also provide three layers of security levels for network communication, and also a mechanism for secure file accesses based on the security privileges assigned to various users is proposed. The files to be accessed from the server are categorized depending on their access privileges and encrypted using a key assigned to each category.*

Index Terms — Biometric, Firewall, One-Time Password, Residential Gateway, SIP (Session Initiation Protocol).

I. Introduction

Over the last couple of years we have witnessed the advent of home network technologies and the proliferation of network-attached devices within home. As more home networks get attached to the Internet with broadband connections such as xDSL, ISDN etc., there is an ever-increasing demand for a secure remote access and control of home appliances from the Internet. The computing resources inside a home or within an organization usually are protected by a firewall to prevent unauthorized access, which does not allow any remote access of home computers unless one uses remote dialing method or Virtual Private network technology. In this paper we are proposing a method that would allow an authorized user to access securely a home network or an organization's computing resources through the firewall.

In particular our design will provide the following four features that are very essential for secure communication between a remote user and the home network or an organization's network and computing resources:

- Secure remote login based on one-time password scheme
- Secure file access based on a hierarchical privilege levels and encryption mechanism
- Secure transmission- contents are transmitted in encrypted form.
- Secure appliance control within a home

Our proposed scheme is based on applying the user's biometrics features together with an encryption scheme to establish a secure communication from a remote machine to a machine within a firewall. Because we are using a combination of both biometrics features and encryption schemes, our proposed design is going to provide more secure way of using remotely a home or an organization's computers.

There has been recently considerable interest to use biometrics features for authentication in a networked society (see e.g., [7], [8], [9] for reviews). The biometrics features of an individual are unique and provide a very convenient method for personal identification. According to [5], p. 4, any human characteristic could be a biometrics provided it has the following desirable properties:

- universality – every person should have the characteristic
- uniqueness – no two persons should possess the same characteristic
- permanence – the characteristic should not change with time
- measurability – it should be possible to measure the characteristic in a quantitative manner.

There are many practical issues involved in developing an authentication scheme using biometrics. Some good pattern recognition algorithms should be developed and used to recognize the biometrics to a very good degree of accuracy (even under "noisy" conditions) and to within a reasonable computer processing time. Also, the biometrics should not be prone to easy tampering by hackers. There are also privacy and network security issues that are involved for developing an on-line biometrics-based authentication system.

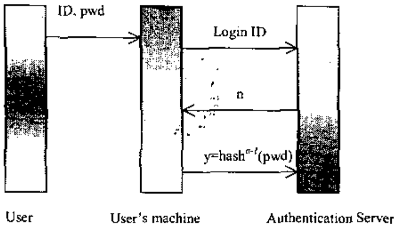
The features that have been commonly used in developing automatic authentication systems are fingerprints, voice, iris, retina patterns, and face. Also, there are some other more unconventional biometrics such as body odors, gait, ear shape, etc. that have been used for developing methods for personal identification. There are several currently available systems for

Mahfuzur Rahman is with the Panasonic Information and Networking Technologies Laboratory, Princeton, NJ 08540, USA (e-mail: mahfuz@ research.panasonic.com).

Prabir Bhattacharya is with the Panasonic Information and Networking Technologies Laboratory, Princeton, NJ 08540, USA (e-mail: prabir@ research.panasonic.com).

Contributed Paper
Manuscript received April 1, 2003

on-line fingerprint verification (e.g., [5], [7]) and on-line signature verification (e.g., [8]). A secure method for accessing files using fingerprints has been developed by one of us recently ([1]). The use of the fingerprints is the oldest biometrics-based method for identification purposes that predates the advent of computer technology.



ID: login ID
Pwd: Password

Steps:
1. Authentication server has a table and every entry in the table contains login ID, n and hash^n(pwd)
2. User logs into its local machine with password and login ID and requests remote access.
3. After receiving a authentication request from the user's machine, the authentication server sends n and ask the user's machine to compute hash^{n-1}(pwd)
4. Authentication server receives y = hash^{n-1}(pwd) from the user' machine and computes hash(y)
5. Authentication server compares hash(y) with the stored hash entry in the table for the corresponding user.
6. If matches then the authentication server replaces hash^n(pwd) with hash^{n-1}(pwd) and replaces n with n-1 at the corresponding user entry in the table of the authentication server.

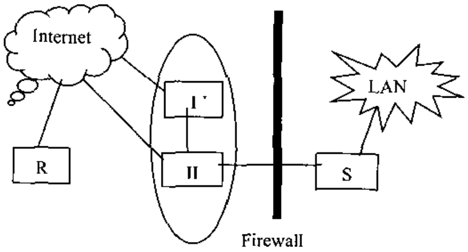
Figure 1: One-time password scheme

The organization of the rest of the paper is as follows. In Section 2, we describe about background technology and section 2 describes remote access scheme. In Section 4, we describe a secure transmission scheme. In Section 5, we describe a secure file access scheme. Section 6 gives our conclusions.

II. Background Technology

A. One-Time Password

The idea of one time password mechanism was invented by Lamport [10]. It is designed to counter the attack of eavesdropping of network connections to get login id and password. In order to use one time password mechanism the user first chooses a password and stores it in the authentication server. The server chooses a number n (something reasonably large) and computes *hash^n(password)* and stores it in its database along with the user id and the number n. The number n represents the number of one time password the user can use i.e., the number of log in sessions the user can have with this password mechanism schemes. If the user exceeds the log in sessions then, he or she needs to initialize again the one time password mechanism with the server.



R: Remote Machine, I: First dedicated Machine
II: Second Dedicated Machine, S: Sever
LAN: Local Area Network

Figure 2 Schematic diagram for Remote Login

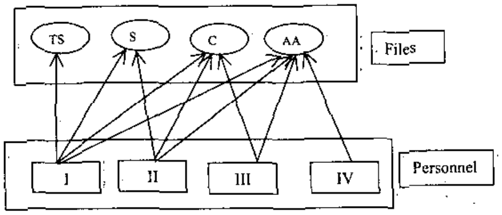
B. Firewall

As computer hacking is quite common nowadays, it is very important to control access to a private network of computers (for example, a company network) – to order to protect the loss of sensitive data to external hackers. A *firewall* is a component or components designed to restrict access to a private network from the Internet (see [3], [13] for surveys). It examines all traffic routed to and from the organization's Local area network to the Internet. It filters out all incoming and outgoing packets depending on the rules that are set by the organization's administration. For example, some organization does not allow any telnet connection coming in from outside and also sometimes they do not allow any out going telnet connection going out of the organization.

These rules can be set based on different network protocols, network address of the destination or source, port number or packet headers etc. Broadly there are four categories of firewalls: packet filtering firewall, circuit lever gateways, application level gateways and multi-layer inspection firewall. The most commonly used method is the packet filtering firewall. Packet filtering firewall (also called as screening router) makes its decision based on the types of incoming and outgoing packets. The main information that a packet filtering firewalls looks at is the following: IP source address, IP destination address, protocol (TCP, UDP, or ICMP packet), TCP or UDP source port, TCP or UDP destination port, ICMP message type Packet size.

III. Remote Access Scheme

The proposed scheme for the remote access will have two dedicated machines outside the firewall to provide secure login. A remote user will communicate with the first dedicated machine outside the firewall before establishing any communication with any machine inside the firewall. The second machine outside the firewall would have a secure connection with the machine/server inside the firewall and would act as a proxy for the first machine outside the firewall (see Figure 2). Our architecture establishes an SSL connection before any communication between an external machine and a machine within the firewall begins. The proposed architecture is further described as follows.



TS: Top Secret, S: Secret, C: Confidential, AA: All Access
I: Category 1(can access all files)
II: Category 2 (can access S, C, AA only)
III: Category 3 (can access C, AA only)
IV: Category 4 (can access AA only)

Figure 3 Hierarchical File Access Scheme

Initially, the remote machine and the first dedicated machine will establish a Secure Socket Layer (SSL) connection. The dedicated machine will then send a request to the remote machine for the user's *strong password* (by a "strong password" we mean the user's password derived from a one-time-password (OTP) and biometrics features). A possible way of implementing this is by setting up a web page that would request for the user's strong password. The OTP scheme will allow the system to use different password each time providing unpredictability and consequent security against any compromise by a hacker. In order to use this system, the user has to initialize the number of OTP's and also a secure pass-phrase into a server inside the firewall. The second dedicated machine is going to act as a proxy for the first dedicated machine and it does not allow any other connection from any other machines. The second dedicated machine is connected to the server inside the firewall using an SSL connection.

After verifying the strong password, the second dedicated machine establishes a direct SSL connection with the remote machine and acts as a proxy for the remote machine for the server inside the firewall. (A less secure way would be to establish a direct SSL connection between the remote machine and the server – this option could be used at the discretion of the organization.) This scheme differs from the AT&T scheme called ABSENT in the following way: we have *two* dedicated machines outside the firewall, and the remote machine communicates only with the first machine which does not have any direct connections with any machines inside the firewall. This arrangement provides less vulnerability a more secure communication link as compared to the ABSENT system.

IV. Secure Transmission Scheme

We use up to three stages of security levels depending on the sensitivity of the protection needed. At the top level, we establish an SSL connection between the remote machine and a machine inside the firewall that might act as a proxy for the server.

In the second level, we use an OTP that changes periodically to authenticate the user's continued presence. For example, after every predetermined interval of time, the dedicated machine inside the Firewall will request an OTP password to check the user's continued presence, and would disrupt the communication if the authentication process fails.

In the third level if desired, we further encrypt the message using a conventional encryption scheme (such as DES, ECC) between the remote machine and the machine to be accessed inside the organization. The key for the encryption is derived using the OTP and biometrics features (such as fingerprints). As the OTP changes periodically, it provides an extra level of security.

V. Secure File Access Scheme

In this section we provide a scheme that would allow an organization to store files in a central directory but the access of those files would be restricted according to hierarchical privilege levels. This hierarchical access scheme could be implemented using the following cryptographic techniques.

We use different secret keys for each file corresponding to each category of access. Two software modules would be used – one running on the server (the machine that stores all the files) and the other running on the user's machine. The server side software module is used to process request submitted by a user to access a particular file and it would verify whether or not that user has the privilege to access that file; then it would send the following message to the user:

$$E_s(k) + E_k(F)$$

where F is the file, k is the secret key used to encrypt the file, s is a key that we refer as the *strong key* - it is derived from the user's OTP password, and biometrics features of the corresponding user, and + denotes the usual concatenation. The client software module receives the message from the server module, and then it decrypts $E_s(k)$ with user's strong password to get the key k, that will be used to decrypt the file. It is also possible to design the client module in such a way so that the files are only readable by the users.

VI. Secure Appliance Control

Figure 4 shows a scenario where a user controls home appliances from a remote location in the Internet. The figure also shows the main components of a home network system: namely a User Agent (UA), residential gateway and a Proxy to the appliances at home. A User Agent (UA) is an end system that acts on behalf of someone who wants to participate in a communication session with the home gateway or with home appliances. In this scenario, a user might be able to control and monitor the home appliances from a remote site. For example, a user while at work realizes s/he forgot to program her/his VCR to record a special show at home. The user formulates and sends a device control message to the VCR to record the program from work. The format of the control command is out of the scope of this paper. For details on control message format see [18]. The proxy at the home gateway receives the message, and forwards it to the appropriate appliance assuming that the appliance is IP-capable, e.g., a PC, and has a User Agent to handle the control requests. If the appliance is not IP-capable and does not have a User Agent, e.g., an X.10 lamp, an appliance controller with a UA must handle the control commands for the appliance. Upon receiving the control commands, the UA executes the control commands carried in the message and forms a response message, which is relayed back to the user. We note that the above scenario is also applicable for the secure access of various devices in an office environment including computers, printers, networked fax machines and coffee makers, etc.

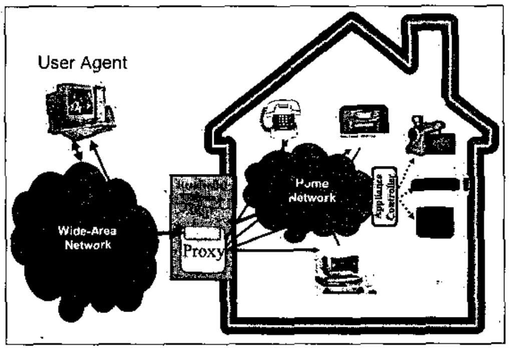


Figure 4: Scenario of Appliance Control

One of the most important issues in relations to appliance control is the authentication mechanism between the agent trying to control the home device and the device being controlled. Authentication is the process of verifying the identity of an entity in a communication session. In a remote appliance control scenario such as the one described above, not only must the appliances authenticate the user but also the user must authenticate the appliances with which s/he is communicating. This is called *mutual authentication.*

It is easy to see why mutual authentication is required in appliance control applications: Firstly, appliances must make sure that only the authorized users are able to modify their behavior, whereas a hacker must be denied access. Secondly, a valid user must make sure that the response that it receives from the appliance notifying him/her of the final status of the control request is actually coming from the appliance. If this step is omitted in the authentication algorithm, then a hacker can receive the request and send a fake response making the user think that the control request has actually finished executing, while in fact the request may have never made it to the appliance at the first place. So mutual authentication is a requirement.

Now that we have shown the necessity for mutual authentication, the next question is how to perform the authentication: We assume that the authentication is based on a shared secret, i.e., a password (one-time). This brings the following question: Should the users authenticate themselves with each appliance at the home network, or should they only authenticate themselves with the proxy running at the home gateway?

Although user authentication with each home appliance has the advantage of providing end-to-end security, it has the following problems:

- An explosion of the number of secret keys occurs: in other words, each (user, appliance) pair must have a shared key to authenticate each other. This results in O(NxM) secret keys and is not scalable (N: number of users, M: number of devices).
- Since some of the home appliances, like light bulb to coffee maker, may be very simple and may not have sophisticated input terminals, e.g., a keyboard, it may not be possible to even set up a shared secret between the appliance and each user that wants to use the appliance. So end-to-end authentication may not even be possible.

The second alternative is to assume a secure home network and have users authenticate themselves with the Proxy running at the home gateway. Although this does not provide end-to-end security and weakens the security model, only one secret key per user must be kept at the proxy, i.e., O(N) secret keys. This secret key could be based on the biometric features and one-time password of the user. This way we could provide a better security model to control appliances from a remote location. We propose to use the second authentication model for appliance control. That is, the Proxy shares a secret key with each user who is allowed to access and control home appliances, and that the mutual authentication occurs between the user and the proxy. Securing the home network can be achieved by employing special packet forwarding policies at the home gateway similar to a firewall and is out of the scope of this paper. We further assume that once users authenticate themselves with the proxy, the Proxy performs access control, i.e., the proxy has an access control database that describes which devices a user is allowed to access and control within the home network.

A. *Protocols for Appliance Control*

There are several candidate protocols for appliance control such as SIP (Session Initiation Protocol) [20], HTTP etc. Also there is always a possibility to use proprietary protocol to carry control commands to the residential gateway from a remote location.

SIP [20] is an IETF standard signaling protocol used for setting up, controlling and tearing down "interactive communication sessions" with two or more participants. SIP sessions include but are not limited to multimedia sessions and telephone calls. SIP is an application-layer text-based client-server protocol modeled after HTTP/SMTP protocols, and is an attractive protocol for appliance control for its simplicity.

HTTP is another candidate protocol for appliance control. Like SIP, HTTP is an industry standard, simple, and text-based protocol. However, SIP is more suitable for appliance control than HTTP for the following reasons:

- A SIP agent has a name-address scheme that is similar to an email addresses. Name address resolution takes place at the last stage, before the device, by a SIP name resolution server that is similar to DNS. On the other hand, HTTP uses physical IP addresses. This makes SIP more suitable in mobile environments.
- SIP is more suitable for event notification scenarios because of the SUBSCRIBE and NOTIFY commands. Event notification is very common in home applications. For example, one may want to receive a notification on his mobile phone if his front door gets opened.

We propose to use SIP as the transport protocol to carry control commands for appliance control. SIP is originally designed for establishing phone calls, its original command set has limited capabilities and is not suitable for device control. Internet draft [23] introduced a new SIP method called "DO". The purpose of the DO method was to enable messages or requests to be sent to networked appliances without setting up a new session [23]. In the case of an existing session the idea was to use the DO method within the context of an existing session, and share the same Call ID as the existing session. However, this proposal has not been adopted by IETF. The current SIP RFC 3261 [20] did not include this extension and also this Internet draft [23] has been expired. In the absence of a separate SIP method for appliance control we propose using the MESSAGE [24] method for appliance control. .SIP MESSAGE [24] method is currently being standardized by the "SIP for Instant Messaging and Presence Leveraging" (SIMPLE) working group of IETF. The purpose of the MESSAGE request is to carry instant messages in the body of the request. For further details on how SIP can carry control commands see [22].

VII. Conclusion

In this paper we have proposed an architecture for secure remote access using one-time password and biometrics features for authentication. We also discussed issues related to secure remote appliance control using our proposed scheme. Also, a hierarchical file-access scheme has been proposed based on user's privilege levels. This scheme uses biometrics features and one-time password mechanism to create encryption keys. For secure transmission of data, we use a three-layer scheme based on SSL connection. The heavy cost of running a VPN (*virtual private network)* (see e.g., [11]) would justify the advantage of our architecture.

References

[1] P. Bhattacharya, "Secure System and Method for Accessing Files in Computers Using Fingerprints," US Patent Application 09/662,298.

[2] J. Bigun, C. Chollet and C. Borgefors (eds.), *Proceedings of the First Intenat. Conference of Audio- and Video- Biometric Person Authentication* ABVA'97, Crans-Montana, Switzerland, Springer-Verlag, Berlin, 1997.

[3] B. Cheswick and S. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, Reading, MA, 1994.

[4] T. Elgamal and K.E.B. Hickman, "Secure socket layer application program apparatus and method". *US Patent 582589*, 1998.

[5] T. Elgamal and K.E.B. Hickman, "Secure socket layer application program apparatus and method," *US Patent 5657390*, 1997.

[6] E.J. Gelb, "Security system for preventing unauthorized communications between networks by translating communications received in ip protocol to non-ip protocol to remove address and routing services information," *US Patent 5550984I*, 1996.

[7] R. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-313, 1997.

[8] R. Jain, R. Bolle and S. Pankanti (eds.), *Biometrics: Personal Identification in Networked Society*, Kluwer Publishers, Boston, MA, 1999.

[9] L O'Gorman, "Fingerprint Verification," in, *Biometrics: Personal Identification in Networked Society*, (Eds. R. Jain, R. Bolle and S. Pankanti), Kluwer Publishers, Boston, MA, pp. 43-64, 1999.

[10] C. Kaufman, R. Perlman and M. Speciner, *Network Security*, Prentice Hall, Upper Saddle, NJ, 1995.

[11] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, vol. 24, no. 11, Nov., 1981, pp. 770-772.

[12] N. Doraswamy and D. Harkins, *Ipsec: The New Security Standard for the Inter-net, Intranets, and Virtual Private Networks*, Prentice Hall, Upper Saddle, NJ, 1999.

[13] V. Nalwa, "Automatic On-line Signature Verification," in, *Biometrics: Personal Identification in Networked Society*, (Eds. R. Jain, R. Bolle and S. Pankanti), Kluwer Publishers, Boston, MA, pp. 143-163, 1999.

[14] W. Shen and R. Khanna (eds.), "Special issue on automated biometrics," *Proceedings of the IEEE*, vol. 85, no. 9, Sept., pp. 1343-1492, 1997.

[15] W. Stallings, *Cryptography and Network Security*, 2^{nd}. ed., Prentice Hall, Upper Saddle, NJ, 1999.

[16] A.E.D. Zwicky, S. Cooper and D.B. Chapman, *Building Internet Firewalls*, O'Reilly, Sebastopol, CA, 2000.

[17] Internet Engineering Task Force (IETF) RFC 2289, "A One Time Password System."

[18] S. Moyer, D. Marples and S. Tsang, "*A Protocol for Wide-Area Secure networked Appliance Communication"*, IEEE Communications Magazine, October 20001.

[19] S. Moyer, D. Marples, S. Tsang and A. Ghosh, "*Service Portability of networked Appliances"*, IEEE Communications Magazine, January 20002.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.