Firewalls for Security in Wireless Networks

U. Murthy[1], O. Bukhres[2], W. Winn[2], E. Vanderdez [3]
[1] Ciber Inc., 8440 Woodfield Crossing Blvd, Indianapolis, IN 46240
[2] Department of Computer Science, Purdue University, Indianapolis, IN 46202.
[3] Lucent Technologies, 2000 N. Naperville Rd., Naperville, IL 60566

Abstract

Wireless computing is an area of computer science that has experienced much growth during the 1990's. The use of wireless networks allows users to access their home networks while separated from them by significant distances. Due to its convenience and the decreasing cost of the needed hardware and software, wireless computing will continue to experience growth into the next century, both in the number of users and in the amount of data transmitted across wireless networks. Along with the growth of trusted users, there will also be an increase in the number of hackers, or rogue users. Due to financial, business, and privacy concerns, it will become increasingly important for system administrators to protect, from rogue users, hosts connected to wire-less networks.

One tool that may be used by system administrators is firewall technology. A firewall allows system administrators to implement strict access controls between the trusted internal network and the non-trusted external world. This paper discusses the firewall and other security tools used to provide security to the wired networks and offers a methodology to protect a wireless network. An Analysis of the proposed methodology and its functionality are also presented.

1 Introduction

The rapid expansion of cellular communications, wireless LANs, and satellite services promises a bright future for users who wish to access data from anywhere, at any time. Users who have portable computers equipped with wireless connections to various information networks are able to perform essentially the same functions as those performed by users on traditional wire-line networks. These wireless networks are linked to the wired networks by one or more stationary host machines, known as mobile host stations MHS, that are capable of transmitting and receiving the signals to and from the mobile users [FZ94] (Figure. 1).

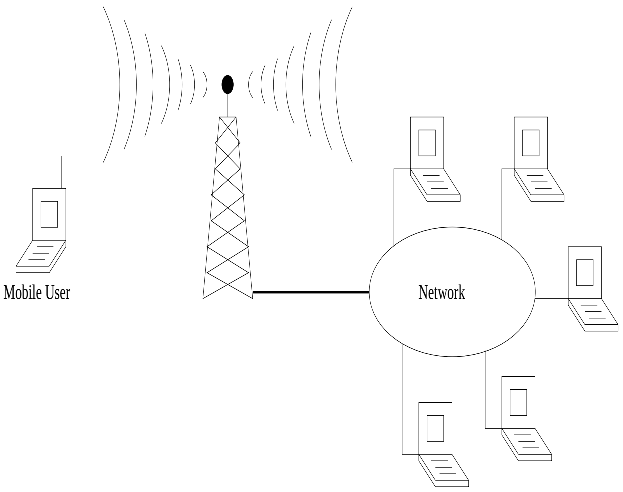

Figure 1: A typical model of a mobile network

Wireless network users do not have the same physical constraints that wired network users have. A wireless network utilizes a wireless communication medium to establish links between the network and its users. This wireless medium allows users to move about freely while they are connected to the network from various locations. In contrast, users of a wire-line network are connected to the network via a fixed switching system and a physical communication medium. This physical medium does not allow for freedom of movement [IB94].

The freedom of wireless network users to connect to their home systems from any place, at any time, does not come without risks. The very medium, which frees users from their homes and offices, increases the security risks of the network. Communication between the network and its users are more easily intercepted; software of malicious intent is more easily introduced into the network; and the network is more vulnerable to attacks by crackers. Many of these problems have been faced in wire-line networks, but the problems are

1060-3425/98 $10.00 (c) 1998 IEEE

compounded in wireless networks.

Additionally, there are many problems in wireless networks that are either nonexistent in wire-line networks, or occur infrequently in them. In a wireless network it is possible for a rogue user to assume the identity of a currently active legitimate user. Once the identity is assumed, there is little current wireless networks can do to detect the rogue user. To compound this problem, mobile computers are more likely to be stolen than their wired counterparts.

Much research has been conducted to protect networks and data from attackers, and even more research is in progress. There are numerous encryption methods that one can use to protect data that are being transmitted. There is research into new protocols for mobile systems that will make machine authentication easier [BCY93, JM96].

The aforementioned ways to establishing network security are necessary but insufficient for protecting a wireless network. System administrators must find ways to reduce the security risks not just to the data being transmitted, but also to the network and to all the hosts that are connected to the network. Firewall technology can help system administrators accomplish this task. A firewall is a hardware or software barrier placed between the network of concern and the rest of the world to prevent unwanted and damaging intrusions of the network [Bryan95].

There has been much work dedicated to firewall and its applications [BC94, CB94, Ranum92, Ranum96]. These works have focused on the area of fixed wire networks. However, at the time of this writing, to our knowledge, there has been no published work on applying firewall technology to wireless networks.

In this paper, we discuss the security concerns of wireless networks and present a method of protecting wireless networks by combining the existing firewall technology and other security devices. The rest of this paper is organized as follows. Section 2 presents the proposed method and section 3 gives a view of related work in this area. Section 4 presents our conclusions.

2 Proposed Methodology

As noted earlier, wireless networks raise numerous issues in the security of networks. These problems stem from three main roots: communication, mobility, and portability. Communication poses a problem since wireless transmissions are more easily intercepted than wire-line transmissions. By allowing users and their computers to be mobile, the risk of a transmission being intercepted is increased. For example, transmissions may have to pass through untrusted or unknown cells before finally being received by the intended end computer.

Portability of equipment allows for more access to computers by potential miscreants by removing the computers from the secure work environment. This places the equipment and network at a higher risk of theft or misuse.

In this section, we address the security problems, discuss the solutions available, and present our solution to part of the problem.

2.1 Identifying and Confronting Security Threats

Security in wireless networks gets more complicated as the privileges of user increase. If the users are allowed to cross security domains, communication may have to be accomplished through insecure channels. If the users are allowed to access privileged services directly (e.g. rlogin, telnet, and ftp), a simple eavesdrop into the connection could supply intruders with enough information to compromise the wireless network being used. Thus, the network should be designed to accommodate various security methods to prevent unwanted intrusions.

Before any security measures may be implemented, the threats to the network being protected must be identified. The threats faced by wireless networks are similar to the ones that confront fixed wire networks and the sources of these threats may be either internal or external to the network. The focus of this paper shall be upon external threats to wireless networks.

After identifying threats to the security of a wireless network, one can then begin to address the problem of system security. The security paradigm may take one of two configurations [Ranum96]. That which is not expressly permitted is prohibited; That which is not expressly prohibited is permitted.

In the former case, the system administrator can define the services that are needed and examine those for security risks. If a service appears to have too high of a security risk, the administrator can easily disallow it. This places the system administrator in a pro-active mode. In contrast, the latter case requires that the system administrator predicts the action that users may take that would weaken system security and disallows those services. This places the system administrator in a reactive mode. Clearly, the first option is the stronger of the two, and it is the paradigm that we have used in our proposed model.

Once the security paradigm has been chosen, the zones of risk to the network must be identified. If the internal network is composed of several machines connected to one another and to an external network, the zone of risk is each node on the internal network (Figure. 2). This requires that each machine connected to the network to protect itself from outside attack.

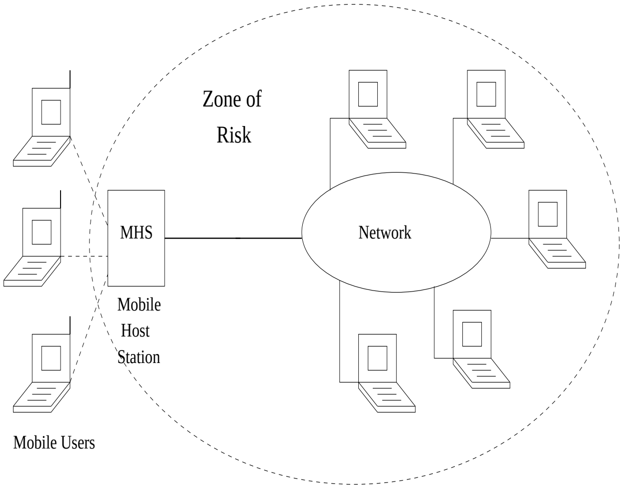

Figure 2: Zone of risk without firewall

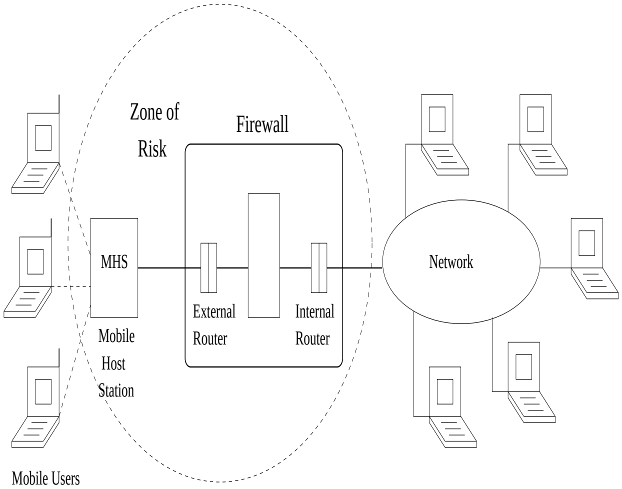

Figure 3: Zone of risk with firewall

The optimal solution is to provide just one zone of risk. This may be accomplished by implementing a firewall system (Figure. 3). This increases network security by reducing the zones of risks from all internal network nodes to the firewall itself. A single, strong defensive gateway is the only point that traffic may pass from the outside world to the internal network, thereby funneling all would-be attackers through one node. This allows the system administration to concentrate upon making one host secure instead of multiple hosts.

2.2 Our Approach

In this section, we explain our method of using Firewalls for providing security to the wireless network. To limit the scope of the paper and as the first step towards the design, the following assumptions are made: 1) There exists a well defined encryption mechanism to protect the data that is being transmitted; 2) The weaknesses or problems faced in the protocols and that arise due to bandwidth used in wireless networks are beyond the scope of our study; 3) There exists a mobile IP addressing scheme; 4) Hosts communicating through any untrusted nodes are not allowed to access any privileged services on the network; 5) The servers, both those operating correctly and those that are corrupt, do not crash. Although, there are techniques to handle crash failures [Reiter94], fault tolerance is beyond the scope of this paper.

Our approach is divided into two parts. First part is the firewall that resides on the wired network side and the second part is the challenge-response system that resides on the mobile computer.

2.2.1 Components and Configuration

In this section, we discuss the firewall that resides on the wired network side. The basic design of the proposed firewall model is shown in Figure 4. The firewall consists of a bastion host and two screening routers. These components share responsibility and work cooperatively to provide security to the network. The router controls network level access whereas the bastion host provides the application level support and protection.

1. External Screening Router:

A screening router is a router that examines packets more thoroughly than regular routers. Most firewall implementations include a screening router. Indeed, the most basic of Firewall design amounts to no more than screening routers.

A screening router can be configured to allow or block packets based on many criteria. In our firewall solution, we configure the screening router to: accept packets transmitted from a mobile system that contains a mobile IP address approved by the internal system administration; accept packets that have, as a target address, valid IP address that are part of the internal network; accept packets that request connections by specifying appropriate port numbers with

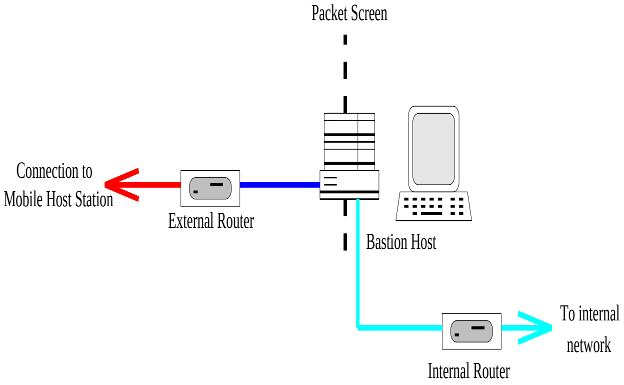

Figure 4: A schematic of our proposed model of a firewall.

respect to the set of rules specified for packet filtering (e.g. TCP port 23 for telnet) [CZ95]; and, Reject packets that are obvious forgeries (e.g. a packet coming from the external world with the source address of an internal host).

The screening router will reject anything not explicitly listed as acceptable.

Although the screening router is a necessary part of the proposed firewall implementation, its limitations dictate that it cannot be the sole component of the design. The rules on which the screening router operates are static and difficult to specify, making administration of the router a challenge. If the firewall is limited to the screening router, the compromise of the router will leave the internal network vulnerable. This violates the concept of "defense in depth." Lastly, the screening router provides no data logging or user authentication capabilities. This is a considerable shortcoming since the ability to log security events and to authenticate users are perhaps the most significant security benefits of a Firewall [Ranum92].

2. The Bastion host:

The weaknesses of the screening router are overcome by using a bastion host in addition to the router. The bastion host provides the link between the screening router and internal router and is the main point of contact to the outside world. The user connects to this host and all the transactions with the internal network are conducted through this host.

In the proposed firewall implementation, we enforce the following rules: i) No user is given an account on this host; ii) Only console login is allowed on this host; iii) All unnecessary applications are removed and unnecessary services are disabled.

In the proposed solution, the bastion host is responsible for receiving and forwarding e-mail, for providing connections through incoming FTP and telnet requests, and for answering DNS queries. A proxy server is executed on the bastion host to implement the packet filtering. The packet filtering is accomplished in such a way that the users can talk to the proxy servers and vice versa. The packet filtering allows the bastion host to accept connections from the users and to respond to the user requests. The number of services and what services should be provided is regulated depending on the network security policy. Thus, the primary function of the bastion host is to act as a proxy server for various services. The proxy server can be implemented by running specialized software for particular protocols or by running standard services for self-proxying protocols [Reiter94].

The proxy server implemented on a TCP/IP network has a problem. In addition to listening to a privileged socket, it also listens to the unprivileged socket and report connection to an inside process. However, in the proposed model, this problem is overcome by an additional IP based packet screening using a secondary screening router between the bastion host and the internal network.

3. Internal Screening Router:

The internal screening router has the same goal, and the same basic functionality, as the external screening router. The internal router protects the internal network from the bastion host and the external screening router. The router is configured to allow a limited number of services to be accessed by the bastion host. This is done to protect the internal network in case the bastion host is compromised.

All screening of data packets from the bastion host to the internal network occurs in the internal router. Since the only communication allowed to cross to the internal network from the external world must originate from the bastion, all IP addresses other than the bastion will be denied delivery.

It should be noted that the internal screening router has the same strengths and weaknesses as the external screening router. In essence, the internal screening router is the last line of defense for the internal network. If it is compromised, the entire internal network is subject to attack.

2.2.2 Smart Cards and Challenge Response

In the first part of the proposed solution, the screening router, which sits on the wired network, verifies that a mobile computer is allowed to connect to the host network by checking the mobile computer's IP address. Since the address is static and transmitted with each communication, would-be intruders could easily intercept the address and configure their machines to use the same legal address. Clearly, an additional form of protection is needed.

The second part of the proposed approach that uses "smart cards" provides the solution to this drawback. A smart card is a credit card like device inserted into mobile computers [Brown95]. Smart cards usually have an independent processor for performing special calculations. In our proposed solution, each mobile computer will be equipped with a smart card that will perform a machine verification function. The verification we propose is a challenge-response mechanism.

In our challenge-response system, the bastion host will issue a "challenge" in the form of a random number. The mobile computer being challenged must reply with the appropriate "response" to continue; otherwise, a disconnection will occur. The response is calculated in the smart card using one or more protected algorithms, allowing the firewall to verify mobile computers. It is important to note that this machine verification goes unnoticed by users.

This machine verification described above will occur at the initial connection to the network. A challenge will also occur whenever a mobile computer is attempting any operations that the system administration determines to be "protected operations" (e.g. FTP, telnet). Additionally, we feel that the firewall should issue challenges at random times. This is to protect the network against a weakness introduced by the wireless medium - the ability for one user to assume the identity of another, currently active user. By issuing random challenges, a rogue user of this nature should be quickly discovered by the firewall.

User authentication is another important security area. Most networks have some form of user authentication as part of system security. These systems usually rely on reusable passwords as the form of authentication. Reusable passwords, however, have an inherent weakness: since users rarely change them, and because they are transmitted over the communication medium, reusable passwords are susceptible to interception and subsequent reuse by rogue users [LL96]. Since the communications medium is more susceptible to eavesdropping in a wireless network than in a fixed wire network, we feel that the risk of reusable passwords are unacceptable. We, therefore, propose the use of a challenge-response system at the user level, similar in nature to the machine verification challenge-response system.

In the challenge-response system we propose, the bastion host will assume the responsibility of user authentication. Each legitimate use of the wireless network will be equipped with a hand-held, cryptographic device, called a token. When a wireless user attempts to attach to the network, the firewall will issue a challenge key to the user. The user will then enter the key into his or her token, which will perform an unknown calculation on the key and answer with the appropriate response, which the user will send as his or her response. Until a user responds, no more operations from that user will be accepted. If the user replies with an incorrect response, a disconnection will occur immediately. This user challenge-response should not only occur upon initial connection to the network, but also whenever a user attempts any operations that the system administration has deemed "protected operations" (e.g. FTP, telnet, etc.).

The machine and user authentication we have proposed should greatly enhance the protection given to a wireless network. The requirement of hidden machine verification allows the system administrator to require verification as often as desired without appearing burdensome to the user. In addition, the use of the smart card reduces the number of computers that can attach to the firewall. Also, since the smart cards are replaceable devices, the system administrator can replace them whenever he feels that the verification algorithm has been compromised. It should be noted that we strongly suggest that the challenge-response algorithms used for machine verification be different than the algorithms used for user authentication. By using different algorithms, one can increase the difficulty for an intruder to pass as a legal user.

The requirement of user authentication is absolutely necessary in a mobile environment. Since mobile computers are at an increased risk for theft when compared to their fixed counterparts, it is imperative that the proposed firewall verifies the users of computers as well as the computers themselves. As with the smart cards, when the system administrator feels the verification algorithm has been compromised, all legal users of the wireless network can be equipped with new tokens.

2.3 Analysis of our Approach

The firewall configuration proposed in this paper should prove to be an effective guardian for a wireless network. There are several advantages in the proposed model. The proposed configuration adopts the concept of "defense in depth," meaning that if one component of the firewall is compromised, there are other components that will stop the intruder, or at least slow the intruder until the system administrator notices the security breach.

The external screening router is the first line of defense. This router will reject all connections, except for those from machines with approved IP addresses. The advantage of this layer is that routers are relatively inexpensive and the system administrator may program the acceptable IP address. The drawbacks of the screening router are that the rules for accepting or rejecting connections are static and that any mobile computer can successfully pass through this router by presenting an allowable IP address as their own.

The next line of defense is the bastion host. This is the single most important component of the firewall. The bastion host performs the tasks of user authentication, machine verification, logging of all security events to an internal host, and execution of proxy servers for all allowed services. The bastion server has no user accounts and the only allowed login is the console login.

The strengths of the bastion host are many, starting with the fact that the security rules need not be static. Since the bastion host is a somewhat powerful computer, it can be programmed to dynamically respond to security events. An example of this in our configuration is the needed user authentication when protected operations are attempted. Another security advantage is gained by limiting the number of services the bastion provides. By doing this, the system administrator needs to ensure the correctness of just a very few programs. Forbidding direct access of the bastion to all users eliminates the risk of users creating security loopholes on it. While the logging of security events does not immediately provide for security on the bastion host, it does provide long-term security by exposing the methods in which rogue users try to infiltrate the internal network.

There are, however, drawbacks to the use of a bastion host on the system. The most serious drawback is the performance capacity of the host itself. If the traffic through this host increases, the system might get overloaded. Thus, this host should be able to withstand a good amount of traffic. However, this can be overcome by having multiple hosts or multiple firewalls.

Another drawback is that users may feel that the host is too restrictive. If this is the case, users may search for ways to circumvent the bastion host. If they succeed, they may expose the network to outsiders. This drawback may be countered by tough corporate procedures regarding the use of the network and by a vigilant system administrator.

A more serious drawback is a problem that is inherent to bastion hosts: if a bastion host is compromised, the intruder (or intruders) has complete access to all processes running on the bastion host. Intruders may plant viruses, open back doors, or re-enable routing between the external world and the internal network, among other things. If routing is re-enabled, the internal network is vulnerable to outside attack. To defend against this threat, we add an internal screening router to the proposed firewall model.

The internal screening router is configured in much the same way as the external screening router. There is one important difference, however: the internal router will accept connections from the bastion host only. This feature gives the network one last line of defense against the external world.

Thus far, the proposed implementation is a fairly standard firewall implementation used by fixed wire networks. However, we are dealing with a wireless network. With the wireless network comes the need to protect against rogue users assuming the identity of currently active users and the need to guard against the danger of mobile computers being stolen. To this end, we add machine verification and user authentication via challenge-response mechanisms.

The machine verification procedure is used by the network to guard against a miscreant user either configuring his computer's IP address to that of a legal mobile host, or a miscreant user that attempts to assume the identity of a currently active user. Machine verification may occur at three times: initial machine connection, attempted use of protected operations/services, and random time intervals. We recommend that machine verification should occur at all three times, including the random interval. By selecting a relatively short amount of time for the random verification, the system administrator can significantly reduce the amount of time rogue users are connected to the system. Also, since the machine verification is invisible to the mobile computer's user, this verification will not be seen as burdensome by end users.

There are two drawbacks to this machine verification procedure. The first drawback is the use of smart cards. Although the price of smart card technology is falling, the integration of smart cards into mobile computers is nonetheless expensive. We feel, however, that system security is worth the cost.

The second disadvantage is again with the use of smart cards. If the algorithms used to correctly respond to a machine verification challenge are compromised, the internal network is vulnerable to rogue users. Smart cards with different algorithms may be issued, but until they are, the network remains vulnerable.

To protect against the above, we suggest that user authentication be performed. The user authentication procedure we recommend guards against the danger of reusable passwords, and are a complementary security procedure for the machine verification. It should be noted that user authentication suffers the same drawbacks as does machine verification (cost and algorithm risk), but there is a synergistic effect when using the two together.

In analyzing our security configuration, it is important to note what we do not address. First, we assume that all data is encrypted using a very secure encryption algorithm. The discussion of encryption techniques is beyond the scope of this paper. Second, we assume that a mobile IP addressing scheme is being used. The discussion of mobile addressing schemes is beyond the scope of this paper. Third, our approach does not take the problem introduced by the bandwidth used in the wireless networks. Last, our system does not protect wireless cells from rogue users. Indeed, we assume that communication cells are full of rogue users and that is why our data is encrypted! Instead, our firewall protects a fixed wire network that allows wireless users to connect to it.

3 Related Work

Wireless networks bring new security issues that need to be addressed by the system administration [FZ94, MDC93]. Mobile computing incorporates new problems since the security of wireless communication may be compromised more easily than wired communication if transmission extends over a large area [FZ94]. The use of wireless networks requires that the issues of connection and disconnection, portability, and crossing service zones be addressed to assure security in the system [FZ94, MDC93]. Additionally, mobile computers raise non-technical issues, such as identity confidentiality, tracking/correlation, and anonymity in foreign domains, that have been studied [HKT94].

Mobile computing requires the creation of new IP addressing schemes. The current IP addressing scheme does not allow for mobile hosts, an essential element in mobile computing. Johnson and Maltz [JM96] and Ioannidis, Duchamp and Maguire [IDM91] have studied the new addressing schemes.

To thoroughly protect a wireless network, transmissions to and from the mobile computers must be protected. Secure communication may be achieved via encryption of transmitted signals [BCY93]. Encryption can be implemented using software, such as Pretty Good Privacy (PGP), or hardware, such as the much-debated Clipper Chip. An authentication mechanism can be implemented using Massachusetts Institute of Technology's Kerberos [BM91, FZ94]. As long as the Kerberos server itself is trusted, it provides a secured authentication without exposing users' passwords on the network. It also allows mobile users to authenticate themselves in unknown domains, thus increasing the scale of mobility [FZ94].

There has been much research and practical application of the use of Firewalls to protect networks from unwanted users [BC94, Bryan95]. Steven Bellovin and William Cheswick of AT&T Bell Laboratories and Marcus Ranum of Trusted Information Systems, Inc. have provided for much of the this research and experience (the experience includes Cheswick's observations of a hacker trying to compromise a firewall [Cheswick92]). Through their work, many types of Firewalls have been developed to enhance the security of networks [BC94, CZ95, Ranum96, and Ranum92]. However, all of the solutions proposed in the literature are directed towards fixed wire networks, and thus fail to properly address the issues that arise from the use of wireless networks. The application of Firewalls to wireless networks is the contribution of this work.

In order to improve on the security provided by adding Firewalls to wireless networks, it is necessary to study the effect of bandwidth and the threats caused by the change in bandwidth. Also it is necessary to implement an authentication method to permit access to only authorized users and machines [BCY93, BM, MST93, Reiter94]. Since these are beyond the scope of this work, our work is based on efficient, existing authentication methods developed by other researchers.

4 Conclusion

Computer usage and the use of computer networks will increase into the next century. As costs for mobile computers and wireless communication decrease, the use of wireless computer networks will increase. Along with the rise in the number of user of wireless networks will come the increased need to protect wireless networks from unauthorized outside access.

Our implementation of firewall technology can play an important role in defending wireless networks from malicious users. By offering just one point of contact between the external and internal networks, the system administrator needs to strengthen just one node against attack. The combination of a bastion host with two screening routers increases the strength of our firewall by adhering to the concept of "defense in depth." The solution put forth in this paper combines several forms of technology – from traditional Firewalls to challenge-response systems – to arrive at a configuration that offers security of wireless networks.

We feel that the key features of the proposed model will provide ability to protect wireless networks from intruders. Key to this is the use of machine verification and user authorization. By requiring the machine and the user to appropriately respond to challenges at key times (and at random times with regard to machine verification), we believe that a high degree of security can be attained. However, there are few limits to the model. The static IP addressing scheme, the performance of the firewall against the growth in the number of users, and the cost of the smart cards are to name a few.

No network that allows contact with the outside world can be made impervious to attacks. Wireless networks are even more at risk of intrusion than wired networks. However, by protecting wireless networks with the firewall implementation introduced in this paper, and by devising and implementing a well designed security policy, attacks upon networks can be made to have minimal effect.

5 References

[AD93] Aziz, Ashar and W. Diffie. "Privacy and Authentication for Wireless Local Area Networks," Sun Microsystems, Inc. July, 1993.

[Aziz93] Aziz, Ashar. "Privacy and Authentication for Wireless Local Area Networks," Sun Microsystems, Inc. January, 1996. vol. 34, No. 1. pp. 56-61.

[BC94] Bellowin, S. M. and W. R. Cheswick. "Network Firewalls," IEEE Communications Magazine, September 1994. pp. 50-57.

[BCY93] Beller, M., L. Chang, and Y. Yacobi. "Privacy and Authentication on a Portable Communication System," IEEE Journal on Selected Areas in Communications, August 1993. Vol. 11, No. 4. Pp. 821-829.

[BM] Bellovin, S. and M. Merritt. "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise," Available through WWW at www.research.att.com

[BM91] Bellovin, S. and M. Merritt. "Limitations of Kerberos Authentication System," USENIX Proceedings, winter 1991, TX Available at ftp.research.att.com.

[Brown95] Brown, Dan. "Techniques for Privacy and Authentication in Personal Communication Systems," IEEE Personal Communications, August 1995. pp. 6-10.

[Bryan95] Bryan, J. "Build a Firewall," BYTE. April 1995. Pp. 91-96.

[CB94] Cheswick, W. R. and S. M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Publications. 1994. Reading, MA.

[Cheswick92] Cheswick, W. R. "An Evening with Berfered," available through FTP at ftp.research.att.com.

[CZ95] Chapman, B. and E. Zwicky. Building Internet Firewalls. O'Reilly and Associates, Sebastopol, CA. 1995.

[Frankel95] Frankel, Yair. "Security Issues in a CDPP Wireless Network," IEEE Personal Communications. August, 1995. vol. 2, No. 4. pp. 16-27.

[FZ94] Forman, G and J. Zahorjan. "The Challenges of Mobile Computing," IEEE Computer, April. 1994. pp 38-46.

[HKT94] Herzberg, A., H. Krawczyk, and G. Tsudik. "On Traveling Incognito," IBM T.J. Watson Research Center N.Y. 10598, USA.

[IB] Ioannidis, J. and M. Blaze. "The Architecture and Implementation of Network-Layer Security Under Unix." Available through FTP at ftp.research.att.com.

[IB94] Imielinski, T and B. R. Badrinath. "Wireless Computing," Communications of ACM. October. 1994. vol. 37, No. 10, pp. 19-28.

[IDM91] Ioannidis, J., D. Duchamp, and G. Q. Maguire, Jr., "IP-Based Protocols for Mobile Internetworking," Proc. SIGCOMM '91 Conference: Comm. Architectures and Protocols, Sept. 1991, pp. 235-45.

[JM96] Johnson, D. B. and D. A. Maltz. "Protocols for Adaptive Wireless and Mobile Networking," IEEE Personal Communications. February, 1996. pp. 34-42.

[LL96] Lin, Ping and Lin Lin. "Security in Enterprise Networking: A Quick Tour," IEEE Communications Magazine. January, 1996. vol. 34, No. 1. pp. 56-61

[Marsh93] Marsh, B. "Systems Issues in Mobile Computing," Technical Report MITL-TR-50-93, Matsushita Information Technology Laboratory, Princeton, NJ. February, 1993.

[MDC93] Marsh, Brian, Fred Douglis, and Ramon Caceres. "Systems Issues in Mobile Computing," Matsushita Information Technology Laboratory, NJ. February, 1993.

[Muffet94] Muffet, Alec. "Proper Care and Feeding of Firewalls," Sun Microsystems, UK.

[Ranum92] Ranum, Marcus J. "A Network Firewall," Digital Equipment Corporation Technical Report. June, 1992.

[Ranum96] Ranum, Marcus J. "Thinking About Firewalls," Trusted Information Systems, Inc. Glenwood, Maryland. Available through WWW at www.tis.com/Home/NetworkSecurity/Firewalls.

[Reiter94] Reiter, M. K. "Secure Agreement Protocols: Reliable and Atomic Group Multicast in Rampart." In Proceedings of the 2nd ACM Conference on Computer and Communications Security. November, 1994.

[Robinson94] Robinson, A. T. "Internet Firewalls: an Introduction," Technical Report. Revision 235. netMAINE, Inc. Portland, ME.

[TW93] Treese, G. Winfield and Alec Wolman. "X Through the Firewall, and Other Application Relays," Digital Equipment Corporation Cambridge Research Lab. May, 1993.

[Weiser93] Weiser, M. "Some Computer Science Issues in Ubiquitous Computing," Communications of ACM. vol 36, No. 7. July, 1993. pp. 75-84.