

MRAS: A Multi-Layered Remote Authentication System

Wilfrid Mirville

Computer Information Technology Department
International College
Ft. Myers, FL U.S.A.

Jamie A. Kobie

Computer Information Technology Department
International College
Ft. Myers, FL U.S.A.

Michael L. Nelson

Computer Information Technology Department
International College
Ft. Myers, FL U.S.A.

Abstract: *Accessing computer resources from off campus has been a continuing problem for both students and faculty, and this problem has been exacerbated by the growth of our graduate program. A multi-layered remote authentication system has been created for use by students and faculty providing the ability to telecommute and gain remote access to these resources. Security concerns have also been addressed regarding unauthorized access to college network resources. This approach could also be ported to most business environments as they share many of the same concerns as our college - providing remote access to users while mitigating potential threats to their networked systems.*

Keywords: user authentication, multi-layer, remote access, secure access

1.0 Introduction

The Computer Information Technology (CIT) Department currently lacks the ability to allow students remote access to projects that are maintained on campus. As a result, students and faculty have resorted to purchasing computing equipment with their own funds in order to have access to the resources needed to conduct activities related to their research efforts and classroom projects. Those that may not have the requisite financial resources, however, are constrained to using the college resources during the hours that the college is open.

The Multi-Layered Remote Authentication System (MRAS) was created to provide remote access to college networked systems while allaying security concerns. MRAS makes use of following technologies:

1. Smart cards are used to authenticate the user both on the user's machine and on the servers involved in the project.
2. Digital Certificates are issued to the user for remote access to the network project server. These are used in conjunction with the smart card as a security enhancement.
3. VPN technology provides a tunneling security protocol that is required when accessing the college backbone over the Internet.

2.0 Background

Multi-layering is one of the more prominent strategies employed in IT security today. Although many organizations have different strategies and are reluctant to divulge the specific methods employed, much of the research suggests that some form of multi-layering is an effective strategy for securing resources from unwanted or unauthorized access. MRAS uses smart cards supplemented with digital certificates and VPN technology to provide a secure environment for remote access to smaller private networking applications.

Access control is often categorized as follows: (1) something characteristic of you - a biometric trait such as voice, iris, fingerprint, palm print, or signature; (2) something known by you - password or PIN number; and (3) something possessed by you - smart card, USB token, identification card. Multi-layered approaches typically involve some combination of approaches from these three categories. MRAS currently utilizes two of these categories (PIN and smart card), but work is underway to include a biometric trait as well.

Another approach to security is often referred to as AAA - access control, accounting, and authentication [1,2]. Access control is a process in which the goal is to limit unauthorized access to the physical or logical network resources. Accounting is a process by which access is tracked by recording usage of network resources by user (not all actions need to be recorded, however the more mission critical systems and devices should be monitored for suspicious activity). Authentication is a process in which the user must present the proper credentials in order to gain access to network resources. AAA is essential in creating a security policy. Access control and accounting can not take place without authentication.

A Virtual Private Network (VPN) is a secure network connection that utilizes existing open distributed public infrastructure. VPNs were originally designed to provide a more economical and scalable site-to-site connection. Unlike a direct connection, VPNs provide a 'private' network utilizing the Internet or public telephone network instead of direct lines. As such it does not require a fixed connection. VPNs provide encryption, authentication, and encapsulation.

VPNs rely on encryption to assure the protection of the data packets and maintain a tunnel. Information can then be extracted from packets using the Certificate Authority (CA). Authentication helps to ensure that the information is indeed from the intended source and no tampering has occurred during transmission. Strong authentication practices are vital since the weakest points of a VPN are at the endpoints. For this project smart cards were used for connection authentication. Encapsulation, also known as tunneling, repackages data packets inside new packets for the journey across a public network. Tunneling strategy is relatively simple in design; instead of packets crossing the Internet out in the open, they are first encrypted for security, and then encapsulated in an IP package by the VPN and tunneled through the Internet [3]. On the receiving end the IP information is removed and the packet is decrypted. The encrypted packet does not have to conform to IP standards since it is encapsulated inside an IP package. VPN security is directly related to the success and strength of the encryption, authentication, and encapsulation processes.

VPN construction typically falls into one of three categories, based on how it is established: hardware-based, firewall-based, and software-based. The choice is dependent upon the level of security needed and the administration resources available on a day-to-day basis. Hardware-based systems are typically encrypting routers used to create a tunnel. These systems typically require IT support but are the most secure option as they encrypt everything. Firewall VPNs such as Cisco PIX Firewall limit access to the network while performing address translation. This satisfies requirements for strong authentication and serves up real-time alarms and extensive logging [4]. Software-based VPNs are software application packages installed on a router, server, firewall, or gateway. This option offers flexibility between different systems and allows selective tunneling protocols to be installed. Unfortunately, the encryption overhead can drastically affect the performance of software-based solutions due to heavy processing requirements [5]. However, software-based VPNs are generally a lower cost option since no new hardware is needed. For this project a combination of hardware-based and software-based VPNs were used. The first VPN was accomplished through Cisco hardware, and the second was software-based through the Microsoft Operating System.

3.0 Challenges

Certificate services and VPN technology took a majority of the research effort. These technologies are time consuming and labor intensive. Microsoft's website contains the majority of the documentation necessary to carry out this project [6]. However, the documentation was at times complex and presented a challenge in terms of navigation. Some of the documentation was difficult to follow when trying to narrow down the exact methodology for deploying the technologies. Finding the right products for this effort was also quite difficult. While much information is available on biometric devices, information on smart card devices was more difficult to find. Also, many sites that offer smart card readers do not carry the smart cards themselves.

4.0 The Multi-Layered Remote Authentication System (MRAS)

The concept of multi-layering remote access connections is not a new concept. This effort differs from other implementations mainly due to the way that it was implemented and the choice of layering techniques. The multi-layering process consists of deploying a double VPN Tunnel and smart card authentication controlled by the Remote Access Server (RAS) running on the Domain Controller.

4.1 MRAS Goals

As previously noted, both students and faculty have extremely limited access to college computing resources. With the exception of e-mail and the college website, access to these resources are subject to the operating hours of the college. The primary goal of this project was to provide a security system that will allow students and faculty to work and manage their projects remotely. Another goal was to allow faculty to remotely administer servers that they set up and may need access to during hours that the campuses are closed.

4.2 MRAS Considerations

Several factors were considered, including the following:

- Server Hardware - must be capable of working with the authentication components.
- Operating System - the selection of operating systems on both the server and client side must be compatible with the server hardware.
- Operating Budget - extremely limited; retired servers were used. Two Athena ASDIIIe Smartcard Reader Starter Kits were acquired for \$230.00.
- Commercial Off The Shelf (COTS) Components - only existing / available components were to be used.
- Connectivity - nothing more than "regular" Internet connectivity should be required.

4.3 MRAS Hardware and Software

Although using existing retired servers is somewhat restrictive, it also ensured that our solution was not dependent upon leading edge hardware or software. For initial testing a Dell PowerEdge 1300/600 and a Dell OptiPlex GX1 550MTbr+ system, both running Windows 2000 Advance Server were used; a Dell Latitude C800 notebook computer running Windows 2000 Professional was used as the client.

Installing the Athena Smartcards was one of the easiest tasks of the entire setup. The drivers and applications were installed, and then each card was customized by assigning new PIN numbers. The only catch was that the driver and application must be installed on the Domain Controller first. Once the cards were customized, a digital certificate was issued to the user of the card.

An enrollment station must be designated for the domain; this can be the domain controller or another server running certificate services. However, there must be at least one server that is the Enterprise Certificate Authority (CA). Typically, only the Enterprise or Domain Administrator should be designated as an enrollment agent. Caution must be taken in issuing enrollment agent certificates - if this account were to be compromised it could have disastrous consequences. According to Athena Smartcard Solutions [7, p. 34], "This certificate is the most powerful of all certificates because an employee with an Enrollment Agent certificate has the ability to enroll for smart card certificates for any domain user, including Administrator." Therefore it is extremely important that the Certificate Service and Certificate Authority are setup correctly. The smart card authentication and VPN (which also uses the smart card) will rely on the Digital Certificate issued to the smart card to authenticate the user.

There are several ways to configure remote access to the network. Most configurations use a single VPN tunnel to provide a secure connection to the network. However, one of our goals was to use layered VPN Tunnels. With layering, two tunnels are used - an external tunnel to connect to the backbone and an internal tunnel to connect to the domain. The external tunnel was established using the college's existing infrastructure (i.e., it was hardware-based). The internal tunnel was created using the Microsoft Remote Access and Routing. Setting up each VPN tunnel was fairly easy. It was, however, important to configure the VPN connection so that the tunnel used EAP (Extensible Authentication Protocol) with smart card authentication. On the client side, using the Microsoft's Make New Connection Wizard, a VPN connection was created for each of the two Domain servers. Just as with the servers, it is essential that the connection settings used EAP for authentication.

4.4 MRAS Testing

Windows 2003 Enterprise Server was initially used on the servers, but during the first week of testing problems arose as they no longer accepted their own certificates as being valid. Several attempts were made to remedy the situation, but when the server ceased to function at all it was decided to change to Windows 2000 Advance Server.

After the failure of the first test using Windows 2003 Enterprise Server, things then went well with Windows 2000 Advance Server. Initial testing involved local authentication. While successful, it led to the discovery that the server's own certificate needed to be added to the Enterprise trust list.

Initial remote testing was also successful, and the server (now running Windows 2000 Advance Server) remained stable and fully operational. However, remote users had access to only a limited number of resources. It was then discovered that the client needed to be on the same domain as the server authenticating the client and the user. Otherwise the user had to be authenticated multiple times to access different resources.

After the success with Windows 2000 Advance Server, Windows 2003 Enterprise Server was reinstalled. Within hours the server began to have problems with both the local and group policies, and would not accept local authentication with the smart cards. As such the decision was made to revert to Windows 2000 Advance Server.

Penetration testing was also done targeting both local and remote access. Although not conclusive, these tests determined the following:

- Clients could not authenticate to the server locally without the smart card and EAP configuration.
- Even though the remote client was within the organization the server was undetectable.
- When given the remote access configuration information the server could not be accessed without meeting authentication protocols and having the required credentials.

5.0 Practical Applications

MRAS should be usable in both the business world and in academia. The use of VPNs is steadily increasing, and this increase is expected to continue [8, 9]. Small and medium sized businesses should particularly benefit from the MRAS approach. Smaller businesses are typically behind the curve when it comes to technology due to cost constraints, ignorance, and/or the lack of technical skills. VPN technology will decrease the cost of networks while enhancing their flexibility and scalability, and at the same time simplify overall network operations. VPNs can be used to extend connectivity to home offices, traveling employees, remote workers, and day extenders [10].

Executives, particularly those in smaller organizations, often have responsibilities that cross many different business aspects and tasks. Remote access provides them the freedom and the ability to reach information as it is needed. It also gives employers several other advantages: access to expertise that is unavailable nearby, the ability to work across time zones at any hour, and it serves as de facto business interruption insurance [11]. For example, a company in London that one of the authors does consulting for was within blocks of the underground bombings that occurred in the summer of 2005. The company employs 20 people, all with VPN connections. Out of those 20 employees only five were in the office that day while the rest were working remotely. As such the company was able to continue working while many other companies spent hours or even days down due to the tragedy.

Many larger educational institutions already use VPNs for student body access. VPN access would also be extremely beneficial to smaller institutions. Smaller institutions often pride themselves on service to their student body. VPN access into the school's servers and applications would assist in the course of studies and enhance the overall educational experience. This is especially the case when the institution or program caters to working professionals and requires project work on a specific server on in a specific application.

However, allowing students access to an educational system can raise various security concerns. Security of the system could be maintained by utilizing smart card technology to limit access to only include those services required by the class(es) that the student is enrolled in. There are many benefits such as 24 hour access, the ability to convert classes that are dependent upon services to an on-line format for distance learners, and more importantly a service to the student body.

6.0 Enhancing MRAS - Where Do We Go From Here

The focus to this point has been on the ability to combine smart card technology with digital certificates and VPN technology to allow a user to work remotely in a secure environment. We have been able to provide a relatively secure and low cost option for remote users. The addition of a biometric layer of security would be an important enhancement, as MRAS would then include all three types of security - (1) something characteristic of you - a biometric trait such as voice, iris, fingerprint, palm print, or signature; (2) something known by you such as a password or PIN number; and (3) something possessed by you such as a smart card. Security audit measures would be another important addition, and there can never have enough testing to ensure security from hackers.

7.0 References

- [1] Fratto, M. "Control the Keys to the Kingdom." *Network Computing*, Sept 2 2002, www.networkcomputing.com/1318/1318f1.html;jsessionid=NJXSEDRMLLTNWQSNDBECKHSCJUMKJVN.
- [2] Shindler, D.L. & Tittel, E. *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress, 2002, www.syngress.com.
- [3] Chae, L. "Virtual Private Networks", *NetworkWorld*, Oct 1 1998, www.networkmagazine.com/article/NMG20000727S0029.
- [4] California Software Laboratories. *Connecting Secured Remote Networks*, Jan 2005, www.cswl.com/whiteppr/tech/connecting_secured_remote_networks.html.
- [5] Andress, M. "Firewall/VPNs: Your Network Dead-Bolt", *Infoworld Test Center*, Sept 29 2000, www.infoworld.com/articles/es/xml/00/10/02/001002esfirewall.html.
- [6] Microsoft Corporation, 2006, www.microsoft.com.
- [7] Athena Smartcard Solutions Inc. *Appendix A: Setting Up a Smart Card Enrollment Station. ASECard Crypto for Windows Integration Guide (Version 3.02)*. Athena Smartcard Solutions Inc., Boston, MA, 2004.
- [8] Friedman, M. "Report: IP VPN Use Will Skyrocket in 2005", *NetworkingPipeline*, Nov 10 2004, www.networkingpipeline.com/security/52600487.
- [9] Wilson, J. "VPN and Security Generating Strong Revenue Growth for Service Providers; Investment in Service Infrastructure Continues", *Infonetics Research*, Press Release, Feb 12 2003, www.infonetics.com/resources/purple.shtml?nr.vpn.security.service.providers.021203.shtml.
- [10] Cisco Systems. *Managed VPN for the Small and Medium-Sized Business*, www.cisco.com/application/pdf/en/us/guest/netsol/ns458/c714/cdccont_0900aecd802402cc.pdf.
- [11] Phelan, S. "Home Is Where the Office Is: CPAs in Small and Midsize Firms Say Telecommuting Is Changing the Boundaries of the Office", *Journal of Accountancy*, 194(6), 2002.