Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
GSEC Certification Paper – Case Study in Information Security

Securing VPN using SafeWord PremierAccess

Claudiu Rusnac
October 12, 2004

Assignment Number: 1.4c

Table of Contents

1.0 Abstract....2
2.0 Before....2
2.1 The Password Problem and Password Testing....2
2.3 Password Risks....3
2.2 The Original VPN Architecture....4
3.0 During....5
3.1 Criteria for Selecting a Two-Factor Authentication Solution....6
3.2 Vendor Selection....6
3.3 Implementing a Two-Factor Authentication System....8
4.0 After....10
5.0 References....10

1.0 Abstract

Virtual private networking (VPN) has become a standard method for users to access corporate resources. Properly securing VPN has become an afterthought. Using a single factor authentication method such as a password can introduce potential risks. These risks include keystroke monitoring, social engineering, sniffing or network monitoring and password cracking. By implementing a two-factor authentication system, an organization can mitigate these risks.

This paper illustrates the problems and risks associated with a single factor authentication system in conjunction with VPN and also how to remediate them. The following are addressed:

- The password problem and password testing
- Password risks
- The previous VPN architecture
- Criteria for selecting a two-factor authentication solution
- Vendor Selection
- Implementing a two-factor authentication system

2.0 Before

After attending the SANS GSEC course it was clear that a simple thing such as a poorly chosen password can create a substantial risk to our organization. The information security team which I am a part of chartered a project to identify and remediate our most critical problem relating to passwords, namely VPN access. Protecting our network perimeter was essential to mitigating potential risks.

2.1 The Password Problem and Password Testing

Key logging software installed on fourteen public internet terminals in the Manhattan area allowed an attacker to compromise personal information and network access from dozens of people and organizations. A company in Silicon Valley endured months of unauthorized access by a competitor before discovering the security breach. [1]

A study done in April, 2004 illustrates this growing problem of password strength. More than 70% of people revealed their computer password in exchange for a bar of chocolate. The study also showed that 34% of respondents volunteered their password when asked without even being bribed. Of those questioned, 80% said they were fed up with passwords and would like a better way to login to work computer systems. [2] The root cause of all these attacks was the password.

Using @stake's L0phtCrack product to test the strength of users' passwords confirmed that our organization was vulnerable and at risk. The test was performed by doing a dictionary attack for a period of five minutes on a 4,500 user database. Within five minutes 992 (roughly 25%) passwords were cracked. Passwords such as "123456", "monday", "friday", "superman", and "sunshine" were among the most common password selections. The most common password discovered was the word "password". These findings pose a serious risk to our organization. Potential risks include an attacker gaining access to our financial systems, customer data and proprietary product data.

A study done by the Secure Computing Corporation [3] also had similar findings:

- Users choose one password for everything. The chances that if an attacker compromises a users web mail password, there is a high probability that the user's network login has the same password.
- Users write down their passwords. Common places where these passwords are hidden are under the keyboard, staplers, or in their desk drawer.
- Users choose passwords they can remember, frequently using personal information such as a family member's name or a pet's name.
- Users also choose passwords such as "stud," "goddess," "cutiepie," or some other vanity word. The most disturbing fact is that users used the word "password" and most of the users who chose it thought they were pretty clever.

2.3 Password Risks

Whether it is a simple password or a complex password both are susceptible to the following attacks:

Password Cracking: Stealing a laptop and attempting unauthorized attempts to login in to our corporate network. An attacker launching and online attack is likely to make a few hundred guesses before he is discovered. An offline password attack can cover hundreds or thousands of passwords every second. [4]

Keystroke Monitoring: Users travel and are often on DSL or cable modem connections. Without proper firewall capabilities, a user's machine can easily become infected with "spyware" that will act as a key logger. An attacker can then use a logged password to attempt unauthorized access into our corporate network.

Social Engineering: “Shoulder surfing” while a user is typing in their password is a common social engineering tactic that can be used. Field users who commonly meet in public places are more prone to this type of attack. Users who volunteer personal information that can seem meaningless are a potential social engineering targets. An attacker can use this personal information to attempt password cracking.

Sniffing or Network Monitoring: Users who use a public internet link such as DSL and wireless are more likely to be targets of this type of attack. Malicious attackers can monitor network traffic and attempt to capture passwords or personal information.

2.2 The Original VPN Architecture

Our VPN remote access gateway was implemented with a Cisco 3060 concentrator. The VPN concentrator is a virtual private network platform designed for large organizations. The concentrator can support high-bandwidth from fractional T3 through full T3/E3 or greater and have up to five thousand simultaneous IP Security (IPSec) sessions.[5] The VPN concentrator provides a 3DES IPSec tunnel into the company’s internal network, allowing users to access network resources remotely.

Our user base consisted of full-time remote users who connected via VPN on a daily basis. This also included users who connected into work using their personal workstation such as IT administrators. In our deployment each user had the Cisco VPN client software installed locally. A VPN profile in the Cisco software defined how the concentrator authenticated. The Cisco VPN concentrator was set up to authenticate users to our division’s Microsoft Windows domain controller (see Figure 1-1). Users would then use their current Windows domain password to access network resources remotely. This provided a simple authentication method. The VPN architecture provided many security features but lacked strong authentication.

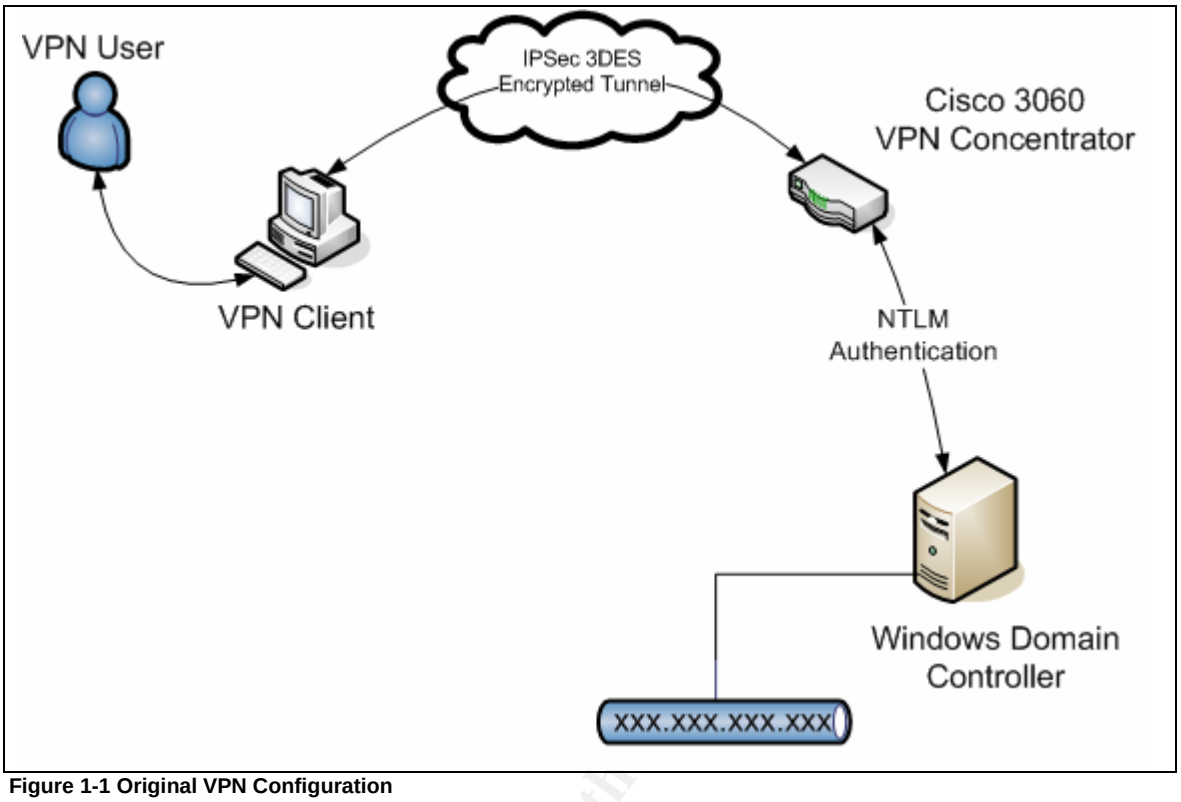

Figure 1-1 Original VPN Configuration

3.0 During

A two-factor authentication system consists of a user having multiple factors: something you have and something you know.

Something you have: Examples are a card key, hardware token or a physical characteristic such as a fingerprint or retina. Physical characteristics are also referred to as "something you are".

Something you know: Examples are password or a personal identification number (PIN).

An authentication system becomes very effective when you combine two factors. An everyday example of a two-factor authentication system is a bank ATM card in conjunction with a PIN. The physical card is something you have and your PIN is something you know. With one of those factors missing, it would be nearly impossible for an attacker to steal money from a bank account. A single factor authentication system is more likely to be compromised by an attack, whereas a two-factor authentication system is less susceptible. Implementing two-factor authentication will mitigate the risks associated with simple password authentication.

3.1 Criteria for Selecting a Two-Factor Authentication Solution

The Sarbanes Oxley Act of 2002 [6] requires publicly traded organizations to implement internal controls that include general computer controls. These controls need to be extensively documented and tested. The information security controls are a key component of the general computer control. The Sarbanes Oxley Act played a crucial role in rolling out a two-factor authentications system. A few security principles we needed to keep in mind while selecting a vendor and implementing a two-factor authentication system included:

Confidentiality: Confidentiality is described as an assurance that information will be kept secret. Examples of confidentiality are encrypting data transmissions and encrypting records within a database.

Continuity of Secure Network Operations: Continuity is described as un-interruption of service or redundancy. An example of continuity is a clustered server environment. Clustering the two-factor authentication servers would allow users to be guaranteed uptime.

Secure Information Access: Secure information access is described as authorization. An example of secure information access is an access control list. A vice president of finance and a helpdesk analyst require different access to different network resources.

Enterprise and Application Level Policy Enforcement: Enterprise and application level policy enforcement is described as systems enforcing the organization's policies and controls. An example of an enterprise and application level policy is a password policy that is enforced by an operating system or an application.

Detailed Auditing Capabilities: Detailed auditing capabilities is described as system accounting. An example is a system logging authentication and authorization access to a system.

3.2 Vendor Selection

The two vendors that our team researched for two-factor authentication technology were Secure Computing and RSA Security. RSA Security sells the SecurID product and Secure Computing Corporation sells the SafeWord PremierAccess product. Both products provide a two-factor authentication solution. Both SecurID and PremierAccess provide support for hardware and software authentication devices.

The SecurID server architecture is a master/slave model, which means that if the primary server is not available, an administrator cannot add or update new records. The slave system is read only. The PremierAccess architecture is designed to be in an all-active cluster mode, that if one cluster member were to go down the other member in the cluster would handle the authentication requests. Administrators would also be able to add and update user records. Another key differentiator between SecurID and PremierAccess is the authentication technology. SecurID authenticators are time based; each hardware authenticator generates a six digit number every sixty seconds. However, a potential problem is the hardware authenticator getting out of sync with the SecureID server. This generally happens over time due to time drift. PremierAccess is an event-based product. The PremierAccess hardware tokens generate random one-time passwords that consist of six alpha-numeric characters. The PremierAccess server expects a block of sixteen sequential passwords; this is done based upon the token serial number. If the token gets out of sync when a user presses the button too many times, the systems will auto-sync itself the next attempt to authenticate to PremierAccess.

The PremierAccess product utilizes the Remote Authentication Dial In User Service [RADIUS] protocol. RADIUS is a protocol that authenticates users on behalf of other services. [7] RADIUS is also a widely supported authentication protocol in networked environments also, a wide range of vendors support and integrate the RADIUS protocol natively. The SecurID requires proprietary integration for devices such as our Cisco concentrator.

The cost models for both products were quite different. SecurID required hardware tokens be replaced every 4 years, unlike the PremierAccess product which licensed the hardware tokens for life. The cost of deployment and maintenance for SecurID is greatly increased due to its license model. SecurID also did not include all components like digital certificate authentication and the web self enrollment server. These features were either not available or were separate costs. The PremierAccess product integrated and licensed both of these features as part of their PremierAccess product.

One key difference and deciding factor between SecurID and the PremierAccess product is that PremierAccess is an AAA [Authentication, Authorization and Accounting] solution. PremierAccess can authenticate and then authorize access to a specific resource. The SecurID product only supports AA [Authentication, and Accounting]. In our organization, an IT administrator and an engineer require different levels of access. PremierAccess allows us to configure users based upon their job function to access different resources.

3.3 Implementing a Two-Factor Authentication System

The two-factor authentication technology our organization chose to implement was PremierAccess. PremierAccess is a solution that is designed to scale with our environment.

PremierAccess can be installed on a variety of different platforms such as Microsoft Windows and Sun Solaris. Our implementation consists of two Sun Solaris systems. The PremierAccess software replicates the user database between the two systems in order to provide redundancy. For additional redundancy systems can be added to the replication cluster. Both systems are active and records can be added or edited on each of the systems. During software or hardware maintenance, this clustered replication allows administrators to take down a member of the PremierAccess cluster and not impact user authentication or updates to the production user database. The Cisco concentrator is configured to authenticate to both systems in case one of the PremierAccess servers is down (see Figure 1-2).

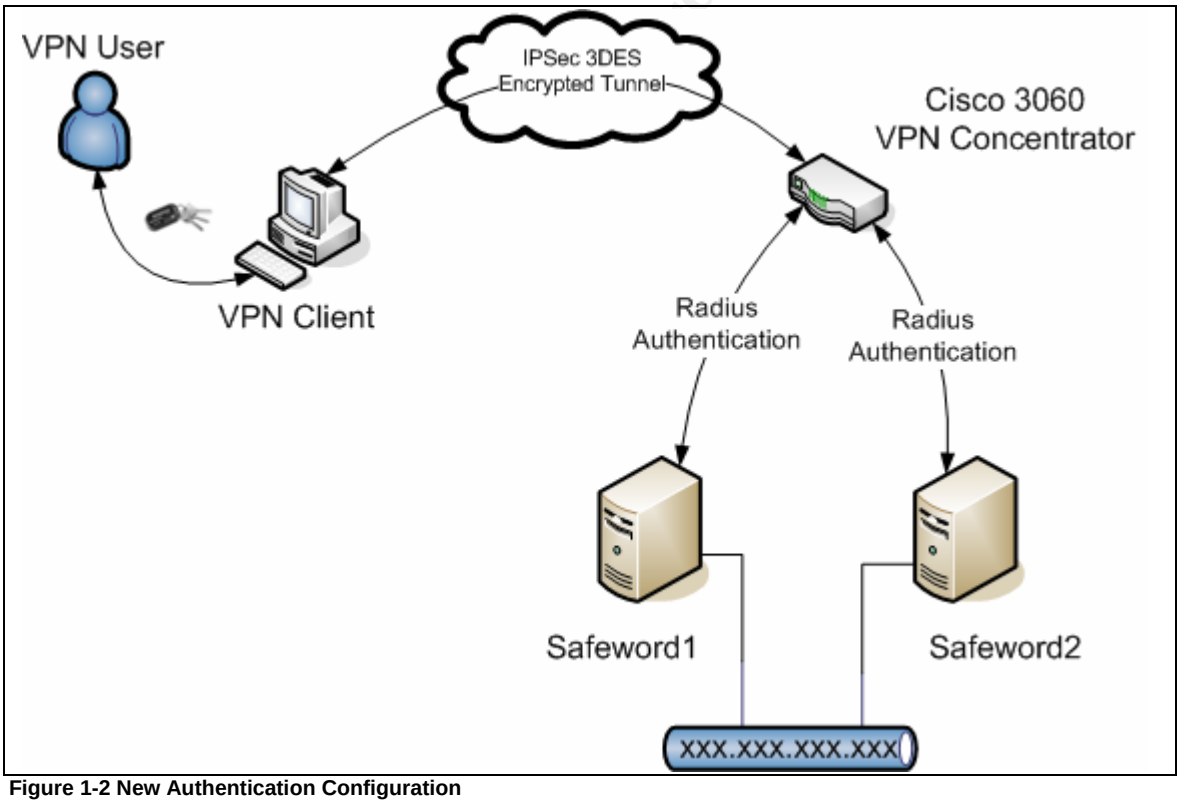

Figure 1-2 New Authentication Configuration

PremierAccess can utilize hardware and software based tokens. A token typically is a hardware device or a key chain fob with a liquid-crystal display that generates a password. When a user is prompted for a password, the user simply presses one or more buttons on the hardware device in order to generate a one-time password. The hardware tokens are programmed to calculate a unique mathematical algorithm which will produce a one-time use password.

Our team chose to implement two different hardware tokens, Silver 2000 (see Figure 1-3) and Gold 3000 (see Figure 1-4). Standard VPN users use the Silver token and IT staff are assigned Gold tokens. The main difference between the Gold and Silver tokens is that the Gold token requires the user to enter a PIN using the keypad to generate a one time use password. The PIN is programmed into the token. When using the Silver token and logging into the system, users append their PIN to the end of the one-time password. If found, the Gold token is less likely to be compromised. After five invalid PIN attempts, the Gold token will display "BAD PIN".

Figure 1-3 Silver 2000

Figure 1-4 Gold 3000

PremierAccess authentication requests are processed through an Access Control List (ACL), which is a collection of rules. ACLs are then assigned to a role, which in turn are assigned to a specific user. The roles are defined by our organizations security policy. By default all users are assigned a "deny" role. This role denies access to any resource unless an "allow" role is assigned.

PremierAccess provides detailed auditing capabilities. An audit log entry is created for every authentication and authorization attempt. This includes successful as well as unsuccessful attempts. Each log entry consist of date and time of the request, whether the authentication and authorization was successful or not.

Logistics is one of the challenges in deploying a two-factor authentication system. Users are now required to carry a hardware token. Assigning tokens individually to each user could be a nightmare! PremierAccess integrated a self-enrollment feature that makes token deployment easier. When users are approved for VPN access, they're assigned to an internal PremierAccess reservation list. The reservation list allows users to be handed a token which they then can activate via a web page. Users are also able to choose a static PIN during this process. The self-enrollment process also assigns the specific user with the proper role that was pre-defined by an administrator. Each member of the PremierAccess cluster has the self-enrollment website loaded which makes this functionality redundant. Once a user completes the web self-enrollment, the token is activated and the user can use it to authenticate. The ability for users to activate and self-enroll reduced the cost of deployment.

4.0 After

The PremierAccess installation provided solutions for our initial problems. The identified risks were remediated with the following changes:

- VPN authentication is now provided by a two-factor authentication system. A poorly chosen password is a negligible risk to our organization
- ACL's were put in place to provide authorization to resources
- Auditing of authentication and authorization requests
- The migration of users to PremierAccess allowed us to implement a process where users are now required to get management approval for VPN access
- Compliance with the Sarbanes Oxley Act of 2002
- IT administrators can disable a user's account for remote access without affecting their local access. This is useful when there is a virus infection and the users home computer is infected, but not their systems at work

The risks that were identified in section 2.3 were a potential risk to our organization. With the implementation of a two-factor authentication system, these risks have been mitigated or completely removed. The new design of VPN authentication was the key solution to removing risks associated with poorly chosen passwords.

5.0 References

1 Secure Computing Corporation. "Weak passwords weaken networks"
URL: http://www.securecomputing.com/index.cfm?skey=1320

2 BBC News UK Edition. "Passwords revealed by sweet deal" April 20th 2004
URL: http://news.bbc.co.uk/1/hi/technology/3639679.stm

3 Secure Computing Corporation. "Weak passwords weaken networks"
URL: http://www.securecomputing.com/index.cfm?skey=1320

4 Tuesday, Vince. "Bad Policy Makes for Weak Passwords" Computerworld Inc. Dec 01, 2003
URL: http://www.computerworld.com/securitytopics/security/story/0,10801,87540,00.html

5 Cisco Systems Inc. "Cisco VPN 3060 Concentrator"
URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2293/index.html

6 Secure Computing Corporation. "Federal regulations / security requirements reference table"
URL: http://www.securecomputing.com/index.cfm?skey=1301#sarbanes

7 Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. Defense in-Depth.
USA: The Sans Institute, January 2004. 156.