Global Information Assurance Certification Paper

Security vs. Convenience

Is RSA SecurID the Answer?

GIAC Security Essentials Certification

Practical Assignment
Version 1.4b

By

Brent Cantafio
April 2, 2004

Contents

Summary

Information Security is a very popular subject these days and many organizations are becoming more aware and diligent with their security practices. Accessing the network has branched out to include VPN and remote access applications, web servers and applications, and more. As security professionals strive to provide these technologies to their end users, they must implement adequate security procedures at the same time. As the stringent access controls and barb wire fences go up to protect the organization from unwanted intruders, the authorized end user often suffers as a result.

This paper introduces the popular security vs. convenience dilemma and examines some of the issues that arise within an organization because of it. In an effort to put the security professionals' standpoint in perspective, this paper provides an overview of some practical security objectives, and discusses the security aspects of both one and two factor authentication. The impact these security practices have on the end user, and on an organization as a whole, is also examined. Finally, a product called RSA SecurID from RSA Security is introduced to see if it can provide the answers, if not a solution, to the security vs. convenience dilemma.

The Security vs. Convenience Dilemma

In a nutshell, the more secure the network, the more inconvenient the access becomes for end users.

The security vs. convenience dilemma has become one of the biggest issues facing information security, with the “lock it all down” mentality present in many organizations today. These information security infrastructures are being modeled after Fort Knox without a single thought given to how it will affect the end user.

For the most part, users want an easy-to-use method to access network resources; they don’t want to be riddled around with complex passwords and security schemes. The security professionals, on the other hand, want to keep the organization’s protected resources safe from unwanted intruders. In essence, they want to make sure that those who are accessing network resources are who they say they are.

As the security professionals proceed with “hardening” the network with stricter password policies, the end user often experiences problems accessing the network. Passwords are forgotten, and in many cases, a complete system lock out will occur after a number of failed attempts. This often causes frustration on the side of the end user as they look for ways to make their access an easier process. The struggle between the two sides will eventually weaken the entire system, as we will examine later.

As new technologies are employed to allow access to secured resources, a method to securely authenticate network access must be implemented to satisfy the security professionals. At the same time, system access must be offered in a convenient and simplified way for the end user. Is it possible for these two contrasting sides to come together in order to reach an effective solution? This may sound like the start of a hopeless task but it is definitely worth exploring.

Before a security method can even be suggested to solve the security vs. convenience dilemma, a closer look at some basic security objectives is needed. Having a better understanding of these security objectives will help clarify what security professionals require, in order to effectively secure an organization’s protected information.

Security Objectives

For users to be able to access protected resources, it must be determined that they are who they claim to be, if they have the necessary credentials, and if they have been given the necessary rights/privileges to perform the actions they are requesting.

Authentication cannot exist by itself; it must be part of a security framework. The four security control objectives that address an adequate security framework are:

- Identification and authentication – to prove identity and allow access to assets;
- Integrity – ensure that data was changed by the authorized person and that no unauthorized changes have been made;
- Confidentiality – restricting data access to the people authorized to see it;
- Non-repudiation – one may not deny his/her actions. [1]

Identification and authentication describe a method of ensuring that a user is in fact, who, he or she claims to be. Once these steps have been completed successfully, the user can access and use the system resources. However, it is also important to track the user's activities and enforce accountability for his or her actions.

By following reasonable security measures, organizations would hope they could achieve these security objectives. However, put a paranoid techie in charge of security and the result would be a complete lock down of everything. Sure everything would be securely protected, but no one would be able to access any information. On the flip side, having an open door approach to security would allow users to access resources quite easily, making for happy employees. The obvious downside to that idea is nothing would be secure, and the floodgates would be open for unauthorized intruders. A little common sense and higher level thinking can help a security professional implement enough security so that user access is convenient and the security objectives are reasonably met.

Password Security

Password security is still, without a doubt, the most widely used method of authentication in organizations today. As security professionals attempt to tighten up the network, the type of password management used will vary in its effectiveness.

Without a strong password policy, passwords are generally easy to guess. End users will often choose a password that has personal meaning to them and is easy to remember. They will often choose words such as the names of their children, pets, sports teams, etc. Easy to guess numbers such as birthdays, phone numbers, addresses are also known to be used. Sure, the end users are content, as they are able to gain network access quite easily. However, this is very close to the open door approach to security, as it leaves very little challenge to today's cyber criminals. By finding out a little information about a person, passwords can be guessed very quickly and an unauthorized user will have access to protected resources.

[1] Curmi. p.1

In a one-factor authentication environment, enforcing a strong password policy is critical for a secure network. The guidelines for a strong password policy include:

- Passwords must change at least every 60 days.
- Accounts are locked after 3 consecutive failed login attempts.
- Passwords must contain at least one letter, one numeral, and one special character.
- None of a user's previous 5 passwords can be reused. [2]

These advanced password policies are often very difficult and inconvenient for the average end user to endure. It is common sense that with the frequent password changes, and the complexity of the password scheme they are forced to follow, more users will encounter problems. With the higher number of users forgetting passwords and being locked out of their systems, there is an added demand on help desks and a loss of productivity.

Is the network really more secure with the enforcement of a strong password policy? The fact is, security professionals can try and follow these best known practices for password security but this usually leads to other problems that, over time, will compromise the system.[3]

To avoid forgetting passwords and being locked out of their systems, some users will write their password down and leave it close to their computer, often pasted to the desk or monitor. This will undermine the whole security process by allowing an intruder easy access to the system and network. "The weakest link in any security system is generally the people." [4]

Even if the end users are educated on their computer responsibilities, the vulnerability to criminal elements still exists. Cyber criminals have developed many ways to hack a password. On the internet today, there are many readily available applications designed to guess passwords by brute force methods. More sophisticated approaches uses electronic sniffers on network lines to monitor the characters being sent. A person could also look over the shoulder of someone typing in his or her password.

These examples represent a small sample of the real-world problems that exist with password authentication. It is evident that using passwords to grant access to protected information leaves us exposed to a variety of security threats. "Passwords are a common form of authentication, yet they are open to a broad array of security problems." [5]

---

[2] SANS Security Essentials – Defense in Depth, p.414
[3] Ohlhorst, p.46
[4] Marshall
[5] Rainbow Technologies, Inc.

A big reason why the security vs. convenience dilemma is such an issue today is because passwords are so widely adopted as a standard for user identification. The security problems already identified with password authentication are what lead to the stringent access controls and big iron equipment, which in turn inconvenience the end user. Hence, the dilemma.

Two-Factor Authentication

Two-factor authentication is simply a more advanced method of password-protecting access to a protected resource. It is comprised of something a user knows and something he or she has. The most popular example used to explain two-factor authentication is the typical ATM banking scenario where you combine something you know (password) with something you have (your ATM card) to prove that you are who you say you are.

Two-factor authentication can also be referred to as strong authentication. Strong authentication can be defined as "systems that require multiple factors for authentication, and use advanced technology, such as dynamic passwords or digital certificates, to verify a user's identity."[6]

This differs dramatically from single password based authentication as the user must provide significantly stronger proof of identity before being granted access to protected resources. The more factors a user must present, the stronger the authentication is considered to be. If your ATM card is lost or stolen, it is pretty much useless without the user's PIN. And, of course, the PIN is useless without the ATM card. It is the combination of both these factors together that significantly increase system security.

In most cases, a PIN or pass code will consist of a four-digit number that a person will keep memorized. It is a lot easier to remember a simple PIN as opposed to a frequently changed 8-character password, comprised of numbers, symbols, and upper and lower case letters. Not only does a simple pass code contribute to the ease of use for the end user; it provides strong authentication when combined with the other factor (something a user has).

The second factor typically refers to something that is unique and hard to copy and often takes the form of ATM cards, smart cards, and tokens. However, the measure of some physical trait like a finger, hand, or eye can also be used and is generally referred to as biometrics. This physical trait can also be used as a third factor (something a user is) to provide even stronger authentication.

Although two-factor authentication provides enhanced security, there are practical tradeoffs. If a person leaves their ATM card at home, or if it is lost or stolen, they will not be allowed access to their money and other banking information. This would cause quite an inconvenience (not to mention a major headache) with many people, as they would either have to go back home to retrieve the card, or contact

[6] Secure Computing Corp.

the financial institution for a replacement. If a similar situation occurred in an office environment, the end user would not be able to access secured resources and the security administrators would need to be contacted for a replacement card or token.

Another tradeoff to this type of security occurs when a user chooses to write their PIN or pass code directly on their ATM card, literally forfeiting the security altogether if the card were to be lost or stolen. As mentioned earlier, when security measures increase, end users will often look for ways to make system access easier for themselves.

Aside from being irresponsible, it is hard to imagine that a person is unable to memorize a 4-digit PIN or pass code, and instead needs to write it down (especially on an ATM card). However, when a person has several of these cards or devices with different pass codes, they become a little more difficult to remember. Writing the PIN or pass code on the cards or tokens themselves is an easy way of dealing with this problem. The risk of someone finding or stealing their ATM card with the PIN written on the back is more than most people are willing to take, as it would affect them directly. Because of the adverse personal consequences, most would choose to memorize their ATM PIN instead. However, one may not think the same way regarding their work smart card or token, as a lost or stolen card would not affect them directly. A user may not view another person accessing network resources with their credentials as serious as the security professionals or the organization would.

New technologies are constantly being developed to tighten the authentication process. These include encryption, digital signatures and access management technology. RSA Security is a leading manufacturer of identity management solutions with a 20-year history of performance and innovation. The company has sales and support offices in all the major international regions and has a solid reputation throughout the information security circle. RSA Security offers a two-factor authentication solution called RSA SecurID, which more than 10 million people around the world now use, according to the company. Several types of authenticators are available to meet the needs of end users, by way of hardware and software tokens. To help shed some light on the security vs. convenience dilemma being discussed, RSA SecurID hardware tokens will be examined in greater detail.

RSA SecurID Hardware Tokens

RSA SecurID Hardware Tokens are authentication devices that are as simple to use as entering a password, but much more secure. These hardware tokens are registered individually to end users, and are used to gain access to protected resources such as VPN and remote access applications, web servers and applications, network operating systems and more.

In short, when a user attempts to access a protected resource, they are prompted for a password. The hardware token generates a simple one-time authentication code, displayed through a LCD window, which changes every 60 seconds. The user combines this authentication code with their secret PIN to create a unique, one-time code that is used to positively identify them. This code is then validated against an authentication server (RSA ACE/Server) to grant or deny the user access.

Three models of RSA SecurID Hardware Tokens are available:[7]

RSA SecurID Key Fob (SD600)

RSA SecurID Card (SD200)

RSA SecurID PINPad Card (SD520)

The key fob and credit card models work in a similar fashion and mainly differ in size and shape. The PINpad differs from the other two models as the user enters their PIN via the 10-digit keypad on the card in order to display the token code. The key fob will attach to a key chain and both the credit card model and the PINpad can even be stored in a user's wallet. Aside from being very portable, all three models are extremely durable.

The RSA SecurID hardware tokens are built on the two-factor authentication approach, similar to the ATM banking scenario mentioned earlier. The hardware token (something you have) displays a different token code for the user every 60 seconds. The token code, combined with the user's PIN (something you know), is what proves that you are who you say you are.

The type of two-factor authentication method used with the RSA SecurID hardware tokens is called time-synchronous authentication. In time-synchronous authentication, both the hardware token and the RSA ACE/Server have internal clocks that are synchronized. Each RSA SecurID hardware token has a built in chip that is initialized with a unique seed when they are shipped by RSA Security. The authentication server also contains this identical seed, which basically, is the starting value both will use in their calculations to produce the token code. The internal chip performs an algorithm, combining and scrambling the seed value and current time, to create a pseudo random number every 60 seconds. This is the one-time authentication code that the user combines with their PIN to prove their identity. The RSA ACE/Server generates the same token code at the same time and stores the seed record on the server. Once the user enters the authentication code along with their PIN, the server matches this value against its records at that point in time. If it matches, the user is granted access to protected resources. [8]

[7] RSA Security Inc. "Hardware Token."
[8] RSA Security – The Power Behind RSA SecurID Two-factor User Authentication, p.2

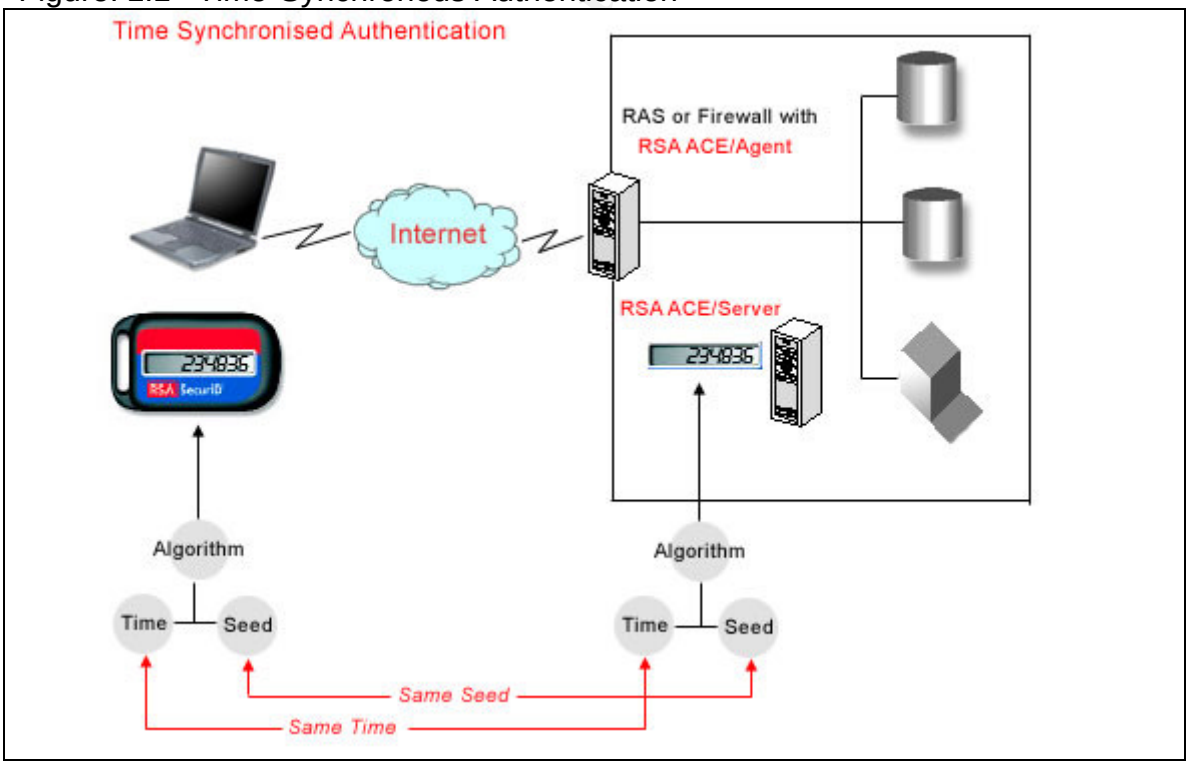
The RSA ACE/Server maintains a log file of all access granted by means of its extensive reporting software. This means that it not only provides secure authentication for its users, but maintains accountability or non-repudiation for them as well.

Time-synchronous authentication proves to be a very effective method of two-factor authentication. It can be broken down in a simple, 3-step process:

1. User enters username and passcode (the passcode is a four-to-eight-digit random token code + the user's PIN.
2. Server and token compute token code by combining seed record and current Greenwich Mean Time.
3. Server authenticates user by matching user passcode with server passcode. [9]

The following diagram (Figure 1.1)[10] about the time-synchronous authentication method illustrates the authentication process used by the RSA SecurID hardware token. It shows that the same time and seeds values exist on both the hardware token and the RSA ACE/Server, resulting in an identical token code when generated by the algorithm.

Figure. 1.1 Time-Synchronous Authentication



[9] RSA Security – RSA SecurID Authentication: A Better Value for a Better ROI, p.1
[10] RSA Security – RSA SecurID Authentication: A Better Value for a Better ROI, p.2

The diagram also refers to the use of RSA ACE/Agents, which function much like a security guard, enforcing security policy as established within the RSA SecurID system.[11] The RSA ACE/Agent technology is built into most leading network equipment, as well as many software systems. The software can provide strong authentication to popular web servers; as well local and remote access on Windows and UNIX environments. The agent software intercepts access requests from users or groups of users and directs them to the RSA ACE/Server for authentication.

The RSA SecurID hardware tokens take advantage of the Advanced Encryption Standard (AES) algorithm, which is today's standard for data encryption. As well, all key aspects of the SecurID solution are encrypted, including user PIN and agent and server communications, to protect against eavesdropping and masquerading. Evasion of attack logic also detects attempted intrusions or use of stolen cards.[12] Security professionals will definitely be pleased with the assurance of knowing that today's high security standards being adhered to by the technology.

Although the RSA SecurID hardware tokens appear to be the end all solution to user authentication, they do have their disadvantages. The first issue is primarily cost. The establishment costs of the RSA ACE/Server and RSA ACE/Agents plus hardware tokens themselves, is somewhat of an investment, depending on the organizations requirements. RSA SecurID hardware tokens must also be regularly replaced and redistributed, often on a yearly basis. On average, the costs to support this type of program are prohibitive for most organizations.[13]

The administrative overhead associated with the planning, setup, and implementation of the entire SecurID solution, is also a consideration, not to mention the honeymoon phase the end users will require along the way. However, any new technology being introduced into a network environment is going to have some degree of administrative overhead and user adaptation. As with many products, once the initial setup is over, it is smooth sailing. The convenience and ease of use the hardware tokens will have as compared to the complex password schemes a user will have to endure, should make it the initial headache worthwhile for everyone.

Another disadvantage is that the hardware tokens can be lost, stolen or left at home, much like the ATM cards discussed earlier. In this situation, the strong authentication method proves very inconvenient, not only for the end user that is unable to access secured resources, but for the security administrator that must assign a replacement token. The end user must always interact with the token, so extra effort is needed on the users' part to include it as part of his or her daily possessions.

---

[11] RSA Security – The Power Behind RSA SecurID Two-factor User Authentication: RSA ACE/Server, p.2
[12] RSA Security – RSA ACE/Server: Enterprise-class security engine for RSA SecurID authenticaiton, p.2
[13] Cryptocard, p.5

Also, as with most two-factor authentication solutions, the system assumes that the user with the hardware token is genuine. If a user were to share his or her hardware token along with the PIN, an unauthorized user may gain authorized access to secured resources by impersonating a legitimate user. An example of this could be if a person forgot their hardware token at home and a co-worker shares their hardware token and PIN with the absent-minded employee. This could also be the case if the PIN was written on the hardware token itself and the device was lost or stolen. As mentioned earlier, the security systems an organization employs are only as good as the people using them.

Without exploring every facet of the RSA SecurID technology, the basic concepts and fundamentals related to the hardware tokens were discussed. As one would imagine, a large number of white papers and articles are available on the RSA Security website (www.rsasecurity.com) that discuss the entire RSA SecurID solution in greater detail. However, for the purposes of offering a solution to the security vs. convenience dilemma, enough information was presented to help make a conclusion.

Conclusions

With today's complex networks, security professionals cannot simply employ the lock it all down approach to security. The end users must be taken into consideration with how security procedures will affect them. For the most part, users want an easy and convenient way to access the network, and security professionals want to ensure this easy and convenient way, is adequately secure.

Organizations will undoubtedly find that the RSA SecurID hardware tokens combined with the RSA ACE/Server will accomplish the security objectives outlined earlier. There is a very high assurance that those persons logging on are, in fact, the authorized individuals, greatly reducing the risk of unauthorized access. However, it was mentioned that when a person shares his or her hardware token and PIN with another person, the security is compromised. The same can be said with any similar two-factor authentication method, and an organization's security policies could help deal with that issue.

The RSA ACE/Server comes equipped with comprehensive reporting features that monitor all access to protected resources. This way, it provides non-repudiation of a user's involvement in any unauthorized activities, which was one of the security objectives outlined earlier that we wanted to achieve.

From the end users standpoint, with the convenience and ease of use of the RSA SecurID hardware tokens, they will be more than pleased. With only a simple PIN to remember, the fewer mistakes and calls to help desk will result in a much happier employee. However, it was mentioned that this is only the case for those that remember to bring their hardware tokens along with them.

Overall, when it comes to balancing security against convenience, RSA SecurID hardware tokens provide all of the key elements to successfully meet a variety of security needs without overly complicating the security process for the end user. RSA SecurID hardware tokens may not be the total solution to the security vs. convenience dilemma but they do provide a healthy balance between the two sides.

List of References

Cryptocard Corporation. "Universal Authenticated Logon." A White Paper. 2003. URL: http://www.cryptocard.com/site/CryptoNew_9/pdf/UnivslAuthLogonWP_030304p.pdf (20 Mar 2004).

Curmi, Julian. "The Importance of a Two-Factor Authentication." Electronic Banking (Part 1). URL: http://www.speedyadverts.com/SATopics/html/information_security1.html (16 Jan 2004).

Curmi, Julian. "Why Strong Authentication is Needed." Electronic Banking (Part 2). URL: http://www.speedyadverts.com/SATopics/html/information_security2.html (16 Jan 2004).

Curmi, Julian. "Token Cards – The most cost-effective solution in e-banking." Electronic Banking (Part 3). URL: http://www.speedyadverts.com/SATopics/html/information_security3.html (16 Jan 2004).

Kibrick, David. "Two-Factor Authentication." 22 NOV 2003. URL: http://security.idlecircuits.com/twofactor.html (14 Jan 2004).

Marshall, Partrick. "CryptoCard lightens security burden." 26 May 2003. URL: http://www.fcw.com/fcw/articles/2003/0526/tec-crypto-05-26-03.asp (14 Jan 2004).

Ohlhorst, Frank J. "Cryptocard solves the security vs. convenience dilemma." CRN. 1066 October 13, 2003 (2003): 46.

Rainbow Technologies, Inc. "Two-Factor Authentication – Making Sense of all the Options." 2 FEB 2002. URL: http://www.itsecurity.com/papers/rainbow2.htm (14 Jan 2004).

RSA Security Inc. "Hardware Token." RSA SecurID. 2003. URL: http://www.rsasecurity.com/products/securid/hardware_token.html (16 Jan 2004).

RSA Security Inc. "RSA ACE/Server: Enterprise-class security engine for RSA SecurID authenticaiton." 2003. URL: http://www.rsasecurity.com/products/securid/datasheets/AS51_DS_1103.pdf (March 20, 2004).

RSA Security Inc. "RSA SecurID Authenticators – The Gold Standard in Two-Factor User Authentication." 2003. URL: http://www.rsasecurity.com/products/securid/datasheets/SID_DS_0103.pdf (16 Jan 2004).

RSA Security Inc. "RSA SecurID Authentication: A Better Value for a Better ROI." 2003. URL: http://www.rsasecurity.com/products/securid/whitepapers/BVBROI_WP_1201.pdf (18 Jan 2004).

RSA Security Inc. "The Authentication Scorecard." 2003. URL: http://www.rsasecurity.com/products/authentication/whitepapers/ASC_WP_0403.pdf (18 Jan 2004).

RSA Security Inc. "Strong Authentication: An Essential Component of Identity and Access Management." 2003. URL: http://www.rsasecurity.com/products/authentication/whitepapers/SA_WP_1103.pdf (18 Jan 2004).

RSA Security Inc. "The Power Behind RSA SecurID Two-Factor User Authentication: RSA ACE/Server" Solution White Paper. 2003. URL: http://www.rsasecurity.com/products/securid/whitepapers/AS51_SB_1103.pdf (17 Jan 2004).

RSA Security Inc. online tutorial. "Using RSA SecurID Tokens for Authentication." 2003. URL: http://www.rsasecurity.com/products/securid/demos/SecurIDTour/RSASecurIDTour.html (17 Jan 2004).

Secure Computing Corp. "Why You Need Strong Authentication." 2004. URL: http://www.securecomputing.com/index.cfm?sKey=647 (14 Jan 2004).

States Services Commission. "6 Approaches to authentication." S.E.E. PKI: Paper 3 - Authentication Mechanisms. URL: http://www.e-government.govt.nz/docs/see-pki-paper-3/chapter6.html (20 Mar 2004).