

## Two-Factor Authentication

### Abstract

Today's widespread use of single-factor authentication is in the midst of change. Both corporate and personal assets are at risk against people trying impersonating users and stealing money and information. Single-factor authentication methods such as the basic username/password combination are no longer sufficient enough.

Two-factor authentication provides a significant increase in security. No longer will an un-secured password provide enough information to a hacker to allow a breach in security. The password or pin number must be used in conjunction the use of tokens, smart-cards or even biometrics. The combination of the two factors will provide companies make sure of the people accessing secure systems.

Roger Elrod  
East Carolina University  
Summer 2005  
DTEC 6870  
Semester Project  
Due: July 17, 2005.

## Table of Contents

Two Factor Authentication .....	3
Introduction .....	3
Single-Factor Authentication.....	3
<i>Problems with Single-Factor Authentication.</i> .....	4
Two-Factor Authentication.....	5
<i>Biometrics used as the Second Factor.</i> .....	7
<i>Pros and Cons of Two-Factor Authentication.</i> .....	10
<i>Two-Factor Authentication in Industry.</i> .....	11
Conclusion.....	12
References.....	15

## Two Factor Authentication

### *Introduction*

If you are walking down the street and you ask for my name, how would you know I am telling you the truth? Well, since you would have no real reason to doubt me, you may just take my word on the matter. But if you were not a trusting soul, you may ask to see some identification. At that point, burden of proof would be on me. I could either decline the offer to prove my identity to you and just walk away, or I could reach for my driver's license. Upon seeing the driver's license, you could either proceed with the conversation believing that my driver's license is real, or, you could just walk away or even report me to the authorities.

The identification process in a face-to-face setting is pretty much that straight-forward. But in this day and age, how many times do we actually meet someone in person and have to wonder if they are who they say they are? Nowadays, more and more people are conducting business in cyberspace.

Corporate networks and the Internet have opened up the opportunity for many lucrative business ventures. The aspect of identity authentication has become of a primary concern for all kinds of businesses.

### *Single-Factor Authentication*

The most prevalent authentication type in use today is single-factor authentication. In short, single-factor authentication is your basic username/ password combination. The single factor in this case is something you know; *your password*. Most business networks and most internet sites use basic username/password combination to allow access to secured or private resources.

*Problems with Single-Factor Authentication.*

How often are usernames and passwords utilized in the daily course of life? At the workplace, employees have to log into their corporate network at least once a day. Some companies still utilize multiple networks. Multiple networks add additional username/password combinations to remember and use. Still many other companies with mainframe capabilities require an additional login credentials. All of the different networks and mainframe's then have different password standards and different lengths of time until the password will need to be changed.

The second 50% of the combination, the password, is the main component of the phrase that is often miss-understood, miss-managed and too often taken for granted. Studies have shown that many users write down their password, choose easily guessed passwords, constantly re-use old passwords and sometimes share their passwords with other people. Technicians often report finding users password on sticky notes under the keyboard, or just stuck on the side of their monitor (Bigler 32).

The Microsoft Corporation has attempted to mitigate one of the inherit problems with the username/password combination. Microsoft has been a proponent of the idea of using "Strong Passwords." Instead of having people use common names for password, Microsoft has detailed the use of using a combination of letters, numbers, and special characters for passwords. While guessing someone's password will be more difficult if the password is "#\$#rU78!", the use of strong passwords will still not deter individuals from writing their passwords down. In fact, the use of "strong passwords" will likely increase the number of times someone jots down their password, just so they do not forget it. (Wildstrom 26)

The common username/password combination is a form of single-factor authentication; the single factor being the password. Another form of authentication, two-factor authentication, is again starting to get noticed in the workplace. The increased use of two-factor authentication is helping to mitigate most of the problems of the basic username/ password system.

If usernames are only utilized in the workplace then that might be something that an individual can handle. However, the Internet has thousands of sites that require even more user name and password combinations. This proliferation of “secure sites” causes individuals to undermine the whole idea of personal security.

Many problems exist within the world of single-factor authentication. The first part of username/password combination, the username, may seem non-threatening in a security sense. However, in a single-factor authentication site, knowing the username, or even the current naming convention of the usernames within an organization already give the potential hacker/thief 50% of the information required to gain access to vital information.

A would be hacker with knowledge of correct usernames can then use specially designed software to try to guess the password. Many people use their pet’s name as a password. Still others use their social security number as their password. While still a few trusting soles use the word “password” as their password. Many programs exist that will easily decipher passwords that use common words or names within seconds.

### *Two-Factor Authentication*

Two-factor authentication provides a significant increase in security over the traditional username/password combination. The two factors of two factor authentication are: something you know and something you have. In the single-factor world of authentication, the password

was the “something you know” part. The additional factor, “something you have”, is the key component.

The something you have component can either be tokens, smart cards, pin/tan’s, and biometrics (to be discussed later).

Tokens display a set of numbers on a small screen. Usually, the set of numbers changes every minute. This number then is joined with the user’s password, or pin number to create a passcode. A correct passcode then authenticates the user to access the secure resources.

Smart Cards are used in combination with a Smart Card reader. The user will insert the card and the card sends an encrypted message to the website or, the reader displays a unique code that the user will enter.

PIN/TAN stands for personal identification number / transaction number. Consumers are provided with a sheet resembling a bingo card that contains many different numbers. Each number is used once to verify a transaction. The PIN/TAN method has grown in popularity in Europe.

Biometric authentication uses biological aspects of the end user, such as fingerprints or iris scans to provide authentication. Other methods of biometrics includes E-signatures and key-stroke dynamics that not only record the final signature or word, but how the signature was either written or typed. (Buss 20)

Immediately one can see the increased security of implementing some form of two-factor security. Since part of the passcode is an ever changing number, the threat of eavesdropping or password interception drops dramatically. Individuals may write down their pin number in order to remember it, however, without the combined number from the key fob, the password becomes useless.

Another side benefit of utilizing two-factor authentication is the decreased load on the internal or contracted help desk. According to the Help Desk Institute, seventeen percent of all calls are from individuals who have lost or forgotten their passwords. People will be less likely to remember a static pin number and these types of calls to the help desk will drop. (Fogarty 68).

*Biometrics used as the Second Factor.*

The use of tokens, smart cards and key fobs are the primary second factor in two-factor authentication. However, as technology advances, biometrics are taking and increasing role to insure the identity of individuals trying to access resources.

“Biometric authentication is the verification of a user’s identity by means of a physical trait or behavioral characteristic that can't easily be changed, such as a fingerprint (Kay 26).”

An alternative to key fobs, tokens or smart cards, using biometrics as a part of two-part authentication is a fairly old concept. While advances in technology make biometrics more conceivable cost wise, adopting this concept still is the most expensive alternative for resource security.

Biometric authentication comes in many different combinations. Seven types that are going to be discussed are signature dynamics, typing patterns, eye scans, hand geometry, fingerprint recognition, voice recognition, and facial recognition.

One of the most popular biometric choices is the signature dynamic authentications. Signature dynamics do more than just record the final image of the signature. This technology also records how the image was produced like the differences in pressure and the speed in which the image was written. Because of the increased amount of variables, the electronic signature is considered unforgeable (Kay 26).

Nationwide Building Society dropped its iris recognition technology in favor of electronic signature pads after observing the results of an in-house study. The study concluded that iris technology could not provide a close enough link between the identification of the person and the completed transaction. Gerry Coppell, Technology Development Controller for Nationwide states, “All the (iris) technology does is to say that ‘that person was standing there in that point in time (E-Signatures 14).

MotionTouch produces the legally-compliant signature technology. The signature pad has the ability to record the X and Y coordinates of the written signature, while also recording the pens pressure. The following biometric data is captured in one signature: speed through the letters, rhythm, direction, flow, pressure, and the final result (E-signatures 14).

Professional forgers maybe able to reproduce the final signature of another individual; however MotionTouch feels that it will be virtually impossible to reproduce exactly how the signature was created.

Trials that included e-signature technology are reporting to show no false accepts or rejects (E-signatures 14).

Another reason why Nationwide switched to e-signatures was the comfort level of the end-users. People are more comfortable writing down their signatures when compared with having their iris’s scanned. Coppell states, “It’s something they’re used to (E-signatures 14).”

Typing pattern technology is similar to signature dynamics. The same way that the e-signature are recorded, typing pattern biometrics record the intervals between characters and the overall speed and pattern of typing.

Eye scans, or iris scans receive a lot of media attention and seems to be the sexy biometric to speak of. Iris scan technology has provided many sub-plots in movies and television.

Many people are uncomfortable with iris scan technology. The ideas of having a laser scan any part of your body, much less and eyeball raises many health and safety concerns. However, these concerns are unfounded, and mostly based on myths.

Iris scans do not use lasers to scan your eyes. A recognition camera takes a black and white photograph and uses a non-invasive, near infrared illumination that is barely visible and very safe (Davis 32).

Fingerprints are a unique biometric that have been used for decades to identify individuals. Fingerprint recognition technology also takes up relatively little space for either the hardware, or the data they capture. However, the general public is uneasy about having their fingerprints captured and stored. Until the general public can overcome this objection, fingerprint recognition authentication devices will remain an option, but not the first choice (Kay 26).

Hand or palm geometry devices are similar take fingerprint recognition devices one step further. These devices measure the entire hand and measure the length and angle of individual's fingers. This method is much more user-friendly than retinal scan devices, however the hardware that supports these devices are bulky and not easily transported (Kay 26).

Voice recognition devices verify the speaker's voice against stored patterns of speech, and facial recognition measures the contours of the face. Features like the outlines of the eye sockets, cheekbones, sides of the mouth, and exact location of the nose and eyes. Hairline

features are usually not examined because of the natural tendency of change in the hairline area (Kay 26).

*Pros and Cons of Two-Factor Authentication.*

While two-factor authentication may seem like the perfect cure-all for securing networks and resources, there are many security holes that this type of authentication will not protect against.

Fake websites provide would-be hackers a way of getting personal information from individuals. The 'store-front' looks authentic, and the user ends up entering information like credit card numbers, social security numbers and bank account information directly into the hands of an identify thief. Two-factor authentication can not protect someone against this type of man-in-the-middle attack.

Another type of security breach is if the would-be hacker already has access the computer itself. Then when the user accesses either company or internet resources, the attacker then attempts to piggyback on the transmission and either perform fraudulent transactions, or access secure resources. Trojan horse attacks like this one also cannot be prevented with two-factor authentication (Schneier 136)

One last factor that may inhibit the introduction of two-factor authentication is the cost. In a two-factor authentication scheme where the second factor is the use of key fobs, or tokens, the costs of those devices alone can be any where between \$75 and \$100 per token. (Wine 13) For a company that employ's hundreds of personnel, this initial cost can be quite high. For a company that has thousands of customers online, the cost of the tokens alone could reach into the millions of dollars. Then there is the cost of the infrastructure needed to support the system. Servers, licensing, Administrators and support personnel have to be compensated, server

hardware must be kept up-to-date, and support costs and product licensing must be paid. At first thought, only companies with deep pockets might be able to afford the ability to use this functionality. However, as Franklin Curtis of Network Computing states, "Every authentication system carries costs, even if you're using the authentication capabilities included in your network operating system or enterprise application.....And even with the simplest authentication schemes, developing a user database, assigning privileges, training and supporting users, and maintenance costs must be factored in." (Curtis 36)

*Two-Factor Authentication in Industry.*

Even though two-factor authentication has been around for decades, its adoption into the business world has been slow. However E-Trade Financial and Bank of America have recently adopted this technology to protect their online customer base.

E-trade Financial adopted two-factor security with a pilot that began in December of 2004. After an initial pilot of 240 users, E-trade is going to offer free authentication tokens for a select group on individuals. Security traders with more than \$50,000 in combined assets, or individuals who regularly trade more than five trades a month will receive these tokens. E-Trade has partnered with Digital Security ID to help implement these improved security standards.

Opponents of implementing token based authentication say that keeping up with the token will be an inconvenience. E-Trade President, Lou Klobuchar states, ""If they care about this, and they want this additional level of security, we're providing them with a solution. If there was no inconvenience whatsoever to using it, it wouldn't be much of a solution. (Trombly: 16)"

Bank of America also has implemented a different form of two-factor security. By year-end 2005, Bank of America will utilize Passmark Security's image-based system called SiteKey.

Gayle Wellborn, B of A's online products and servicing executive, states that while this additional security will start out as an option, eventually, this will become mandatory for all of their 13.2 million online banking customers (Will 7).

B of A is implementing this additional technology in response of a lawsuit by a Miami businessman. A cyber criminal from Latvia used a key-logging program to get account information from the business owner, and used that information to get \$90,000 wired to his personal account (Trombly 24).

Instead of using a token and randomly generated numbers to authenticate to the banking network, customers will enroll into the system by picking an image they will remember, writing a phrase, and then selecting three challenge questions (Will 7).

On future visits, the customer will enter their user name and then the image they selected will be displayed on the screen, along with the phrase they input upon registration. The image and phrase will then confirm to the user that they are on an authentic B of A website, and not a counterfeit site (Will 7).

Avivah Litan, a vice president and research director at Gartner Inc. in Stamford, Conn., said she has been recommending the imaged-based concept to banks, stating that the Passmark Security concept is a very practical method for implementing mutual, two-way, two-factor authentication (Will 7).

### *Conclusion*

Heightened security methods are here to stay. Some companies are trying to increase their own security by tightening existing password policies. To increase security at a company to remain nameless, these following rules were implemented:

Table 1:

Example of One Companies attempt to secure a username/password combination

Password Expiration	No Shorter than 90 days
Password History	Enforced for five iterations
Password length	Six to eight characters
Password Composition	One lower case letter One number NO special characters
If the password needs to be written down	Should be done in a secure manner.

Note: Date taken from “Password Standards Can Improve Agency Workflows and Carrier Security.” By Alvito Vaz

Security cannot be taken for granted. Security ‘improvements’ like the ones stated above illustrate the fact that the people making these ‘improvements’ do not have any idea about true security features.

Passwords that expire no sooner than 90 days are susceptible to eavesdropping. Having a password history of only five iterations increases the ability to guess passwords through pattern matching. Password lengths of a maximum of eight characters are not long enough. By not allowing special characters, the password can be easily guessed. Lastly, there is actually a policy in place about how to write down passwords.

Most companies, 87% according to a recent study, rely solely on user identification and passwords for authentication. Even though still in their infancy, the use of tokens, smart cards and biometrics drop unauthorized access breaches drop from typically to just 3% (Hackers 32).

Companies will slowly realize that addition security features will be required. Two-factor authentication will slowly be adopted into mainstream corporate America. More and more, companies will implement some of the authentication methods discussed here. However, what about the future? If the token-based method of authentication goes into critical mass, there could be a time where individuals have to keep up with multiple tokens for different logins.

RSA Security already has a process in place to combat the overuse of token-based authenticators. Currently, companies using RSA technology have internal servers providing the authentication against the random numbers produced by the tokens. The service that RSA can now provide would authenticate an individual's token against RSA host servers. This will allow individuals to and from RSA secured sites without having to maintain multiple tokens (Wolfe 1).

While two-factor authentication will have to undergo a ramp-up period of any number of years for the general population to grasp, the online threats to both personal and business assets and resources will only increase over time. Tokens, smart-cards, and biometric authentication methods will become as common place soon as the regular ATM and pin numbers are now.

Table 2

Company's Specializing in Two-Factor Authentication

ALADDIN	Arlington Heights, ILL	<a href="http://www.ealaddin.com">www.ealaddin.com</a>
AUTHENEX	Hayward, Calif.	<a href="http://www.authenex.com">www.authenex.com</a>
RSA SECURITY	Bedford, Mass.	<a href="http://www.rsasecurity.com">www.rsasecurity.com</a>
SECURE COMPUTING	San Jose, Calif.	<a href="http://www.securecomputing.com">www.securecomputing.com</a>
VASCO	Oakbrook Terrace, 111.	<a href="http://www.vasco.com">www.vasco.com</a>
VERISIGN	Mountain View, Calif	<a href="http://www.verisign.com">www.verisign.com</a>

Note: Data taken from "Another Obstacle for Hackers to Scale", by Elizabeth Wine.

## References

- Bigler, Mark. "Single Sign On." Internal Auditor December 2004: 30-34.
- Buss, Dale. "Two Factor, Too Tough?" Securities Industries News June 6, 2005: 16-20.
- Curtis, Franklin. "Strong Authentication" Network Computing February 3, 2005:34.
- Davis, Russ. "Giving Body to Biometrics." British Journal of Administrative Management April/May 2005: 32-33.
- "E-Signatures Win Over Iris Scans." IEE Review January 2003: 14.
- Fogarty, Kevin. "Paying Less for Passwords." Baseline December, 2004: 68.
- "Hackers Sharpen Their Blades." Management Services May 2004: 32-33.
- Kay, Russell. "Biometric Authentication." Computerworld April 4, 2005: 26.
- Schneier, Bruce. "Two-Factor Authentication: Too Little, Too Late." Communications of the ACM April, 2005: 136.
- Trombly, Maria. "Bank of America Moves to Strong Authentication." Securities Industry News February 28, 2005: 24.
- Trombly, Maria. "E-Trade Rolls out Two-Factor Identity Check." Securities Industry News March 7, 2005: 16.
- Vaz, Alvito. "Password Standards Can Improve Agency Workflows and Carrier Security." National Underwriter / Property & Casualty Risk & Benefits Management Edition June 9, 2003: 23-25.
- Wildstrom, Stephen. "Securing Your PC: You're On Your Own." Business Week May 26, 2003:26
- Will, Wade. "B of A to Use 2-Part Verification." American Banker May 31, 2005: 7.
- Wilson, Jeff. "Enemy at the Gates: The Evolution of Network Security." Business

Communications Review Dec. 2004: 14-18.

Wine, Elizabeth. "Another Obstacle for Hackers to Scale." Treasury and Risk Management

June 2005: 13.

Wolf, Daniel. "Weighing Costs, Potential of 2-Tier Security Devices." American Banker March

2, 2005: 13.

Wolfe, Daniel. "Two-Step Log-ins Push Aggregators to Adjust." American Banker June 8

2005:1-2.