Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust IdentityGuard for Microsoft Windows

February 2005

Entrust®
Securing Digital Identities & Information

Table of Contents

1 Executive Summary

By adding a second factor of authentication to a Microsoft Windows desktop, Entrust IdentityGuard™ Client for the Microsoft Windows platform can make it possible for your organization to provide stronger assurance, that users are indeed who they say they are, before granting them access to the Windows desktops, corporate network and the valuable resources it contains.

This second factor of authentication adds security to the desktop itself as well as to the corporate network when users are connecting directly, over wireless networks, or over the Internet with or without a VPN.

Without a second factor to authenticate users, organizations are subject to the security weaknesses associated with simple username and password authentication.

2 Introduction

When logging on to their desktop, users not only have access to the resources and information stored on the computer, they also effectively open a door to the corporate network, and its resources including all the sensitive data and applications. As users become more mobile and require access to the corporate resources from anywhere at anytime, the door to the corporate network can effectively be opened from a wired or wireless connection to the local network or from the Internet

The security of the desktop and of the network itself is only as strong as the methods used to identify the users logging onto devices and granting access. Organizations need to consider increasing the protection of their corporate resources by improving the mechanisms for user authentication.

A compromised desktop or laptop may not only contain highly sensitive data that relates to company secrets, employee or customer information, personal privacy or regulatory requirements, it can also provide unauthorized access to the entire network.

In a recent research note Gartner states that “The threat of unauthorized access to corporate networks has increased due to widespread Internet access. Employees are requesting corporate network access via many devices, including laptop computers, personal digital assistants (PDAs) and Internet-enabled mobile phones. Some companies also allow external users, such as business partners, customers and suppliers, to access their networks, which increase the risk of external attacks.” [1]

Given the proliferation of vulnerabilities and attacks, organizations must protect themselves against the threat of illegitimate access to corporate networks and systems locally or over the Internet. Since users now access the corporate network via a number of connection options – wired, wireless, dial-up, VPN, or over Terminal Services - the threat isn’t just from attackers impersonating users with local or remote access. Anyone who gets access to the network from the Internet can attempt to impersonate any legitimate user.

Unfortunately the threat isn’t limited to external users. Gartner estimates that more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses. The U.S. Treasury estimates that 60 percent of financial-institution intrusions are committed by employees.

Basic Microsoft Windows desktop authentication uses a username and password to identify users. Usernames and passwords are a single factor for authentication – *something you know* – and considered to be one of the weakest forms of authentication used today.

The more difficult it is to impersonate a user by forging or faking the means of authentication, the stronger the authentication mechanism is. Adding a second factor to the user authentication process – *something you have* –helps to provide a higher level of security that is better suited to identify users.

[1] Gartner, Assess Authentication Methods for Strong System Security, August 2004

3 Strong Authentication

3.1 Passwords are not enough

Password-based authentication mechanisms contain a number of inherent security weaknesses. Compromised passwords are among the most common security vulnerabilities to systems that base user authentication on this single factor. Users are often careless with their passwords and password policies are difficult to enforce. Attackers have plenty of tools for defeating password protection and these can be both technical and social. Once an attacker has a user's password, he has the means of accessing the rightful user's privileges. If such user has access to corporate resources, the attacker can access those same resources as they log onto the Microsoft Windows desktop and network.

The selection of a weak password is one of the most common security vulnerability and is likely to be a primary source of security breaches. Adding strength to the password such as increasing its length or including special characters will somewhat mitigate the risk, but tools are readily accessible to compromise strong passwords. The following are some of the most common threats and attacks on password security:

Lack of user care can lead users who have multiple passwords to write the passwords down on paper or other readily accessible media.

Poor password selection such as a favorite pet's name, leaves passwords vulnerable to guesses and dictionary attacks. Password guessing involves entering common passwords either manually or through programmed scripts.

Shoulder surfing occurs when someone reads a user's password as it is being entered.

Social engineering an analysis of attacks demonstrates that it is still surprisingly easy to obtain users' passwords simply by asking for them. Social engineers masquerade as administrators or another authoritative role to convince users to tell them passwords.

Brute-force logon attacks follow the same basic logic as password guessing but are much faster and more powerful. Very large dictionaries and user lists are used as tools to automate the process. Brute-force attacks are more efficient than password guessing, however both techniques are essentially the same.

Keystroke logging uses desktop tools to record user keystrokes as they enter information, including usernames and passwords.

4 Adding factors for stronger authentication

Given the number of very real threats and proliferation of attacks on Microsoft Windows desktops, organizations need to improve their user authentication processes by deploying tools that allow users to be identified with *something they have* in addition to *something they know*, such as a password.

Adding a **second factor for authentication** in which a user has physical possession of the object or authentication device to be granted access can enhance security. Gartner states that "Two or more authentication factors — something the user is, has or knows — are necessary to grant secure system access in mobile environments"[2]. Examples of second factors for authentication range from magnetic and radio frequency (RF) cards to smart cards. Also included in this category are one-time password tokens, USB tokens, and digital certificate/private key pairs.

When considering a second factor of authentication, organizations tend to look for a solution that is inexpensive and easy to deploy. In addition, the authentication device itself should be resilient and robust to help prevent ongoing capital and management costs associated with alternative second factors of authentication products such as hardware tokens that inevitably have to be replaced over time.

Forrester recommends that ***"Firms that need (second factor) authentication but find hardware tokens and smart cards too costly and complex***

[2] Gartner, "Mobile Authentication Yields Anytime, Anywhere Control", October 2004
[3] Forrester (Jonathan Penn), *Strong Authentication Made Simple*, November 2004

should consider piloting Entrust IdentityGuard."[3]

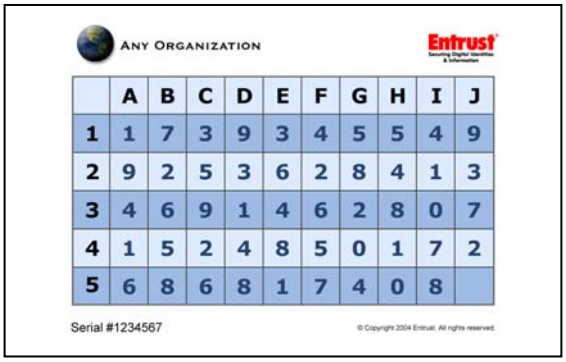
5 Entrust IdentityGuard™ – Simple and Cost Effective Security

Using a patented challenge and response technique, Entrust IdentityGuard™ Client for the Microsoft Windows platform provides a stronger second factor of authentication, improving the security of desktop authentication, thereby significantly increasing resistance to password attacks on the Microsoft Windows desktop. Entrust IdentityGuard Client for Microsoft Windows has been designed with the real-world demands of strong authentication in mind while taking into account ease of use, deployment and management costs.

5.1 Stronger, Yet Simple, Authentication

Entrust IdentityGuard Client for Windows provides a stronger second factor of authentication for a Microsoft Windows desktop. As discussed earlier, one of the most effective ways of mitigating an attack on a Microsoft Windows password is to make it extremely difficult for attackers to impersonate users. The Entrust IdentityGuard solution can make this much more difficult to achieve.

With the Entrust IdentityGuard solution, the user continues to employ their current user name and password to logon to Microsoft Windows but the user is also provided with a second physical form of authentication based on a random assortment of characters in a grid format printed on a card. An example of this grid is shown below:



The format of the grid is very flexible. Contents could be numeric, alphanumeric, etc… depending on the application requirements. What is important is that each user has a unique randomly generated grid that they will use for authentication.

To authenticate themselves, users would first employ their user name and password to logon to Microsoft Windows as usual.

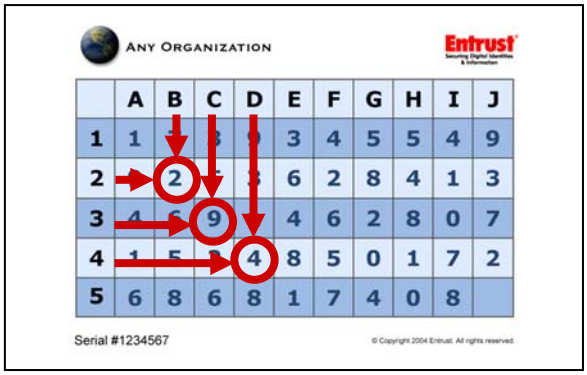
If the proper user name and password is submitted for Microsoft Windows authentication, Entrust IdentityGuard Client for the Microsoft Windows platform would then prompt the user to respond to a coordinate challenge that would then be used to demonstrate they are in possession of the appropriate IdentityGuard grid.

The displayed challenge is locked and will not change until successfully completed, or, alternately the user can be locked out of the Windows desktop for a designated amount of time after a pre-set number of unsuccessful attempts are made in responding to the challenge.

The challenge is associated with the specific user account, based on the first step of authentication – the Windows username and password. The challenge is not changed if the dialogue is refreshed. This approach can help prevent an attacker from cycling through different challenges to obtain one that may be more appealing. Once the user successfully completes both steps of authentication, the challenge is updated using the random number generation capability of Entrust's FIPS 140-2 - certified cryptography.

It's important that the second factor of authentication be available both online as a user logs onto the corporate network, and offline when mobile users are logging onto their standalone desktop without any connection to the corporate network. As such, Entrust IdentityGuard Client for the Microsoft Windows platform will challenge the user with a grid response both online and offline to help maintain authentication security.

In the example above the user is challenged by IdentityGuard Client for the Microsoft Windows platform using grid coordinates *B2*, *C3*, and *D4*. The user would then refer to the Entrust IdentityGuard grid and respond as follows:



Similar to a *Bingo* card or map location look up, the user would respond with the grid cell contents that correspond to the challenge coordinates. In this example, the user would enter the grid locations for location *B2*, *C3*, and D4 - "2", "9", and "4". For each subsequent login, a different random challenge would be generated and the user would be prompted for the appropriate response.

Thus, the user has a second factor for authentication with a one-time challenge and response mechanism that is designed to be resistant to fraudulent impersonation. Even if an attacker successfully tricks a user into attempting a login in order to steal the response, the attacker will only gain knowledge of a single challenge/response set. If an attacker proceeds to use it to gain access to the Microsoft Windows desktop on another occasion, they would be confronted with a new random challenge for which they would not have the correct coordinates.

On a 5 x 10 card as shown in the example above, there are 19,600 unique three-coordinate challenge sets. This is in sharp contrast to user name and password alone where one single successful attack will result in the user's Microsoft Windows credentials being stolen.

Entrust IdentityGuard provides security that is easy for a broad range of users to use. The grid lookup concept used by the Entrust IdentityGuard solution leverages ubiquitous experiences. Users will be familiar with this grid type concept from games like *Bingo* and *Battleship*, or from looking up locations on a map. This means that very little user education is required for the solution to be successfully used.

Further, the form factor of the Entrust IdentityGuard grid fits better into real-world deployments. The grid can be deployed on a wallet-sized plastic card or on the back of a personnel identification badge, for example, which fits with a user's current authentication habits: it is easy to carry around and very durable. While conventional hardware tokens rely on the technology within the hardware device, that is often powered by batteries or at times may be faulty when subject to physical abuse or colder climates, Entrust IdentityGuard grid cards are much more immune to the regular day to day physical abuses are inevitable.

5.2 Resistance to More Sophisticated Identity Theft Attacks

Entrust IdentityGuard helps to reduce the susceptibility of repeated password attacks. A user could be subject to more sophisticated attacks than simple social engineering, shoulder surfing or password guessing. In a Trojan attack, a piece of malicious code such as a keystroke logger is installed on the end user's computer and scans the users actions such as their keyboard strokes. User names and passwords could be stored locally and later sent over the internet to the attacker. While firewalls, anti-virus and anti-spyware software reduce the odds of such malicious software being installed on a user's computer, there will be a certain number of users who will not have the latest security software.

Because of the large number of potential challenge and responses for any given user, even attacks that record several logins will only be exposed to a small portion of the Entrust IdentityGuard grid. To further provide consistent and stronger security, users could be periodically reissued with replacement cards containing all-new random grids. As there is no specialized hardware requiring distribution, it is more cost effective to replace these cards periodically to enhance the level of security .

A flexible card format allows security to be readily tailored for customer requirement. The security of the Entrust IdentityGuard grid can be increased by changing its format. The most significant impact to security is achieved by modifying the number of grid cells. By increasing rows and/or columns in the grid, security can be increased in a linear fashion. For example, doubling the number of grid cells can at least double the security. The other characteristics of the card format impacting security is the entropy of individual cells. Increasing the number of values in an individual grid cell can increase security, but to a lesser extent than increasing the number of cells. For example, moving from a single alphanumeric character to a double digit number effectively increases entropy by approximately three fold. However, the actual security improvement is only about 10%.

For most deployments Entrust recommends a 5 x 10, single character card. This provides a good balance between security and usability. Entropy of the card is high with over 10^{67} different unique grids. As the examples herein demonstrate, a 50 cell grid is also very legible. The result is security that is over 100 times more resistant to attacks than passwords alone.[4] For most users, this means that each grid can be deployed and used for a year or more.[5]

Another element to be considered in deployment is how many cells are prompted for in the authentication challenge. The shorter the challenge, the more susceptible it is to a brute force attack but the easier it is from a usability perspective. The longer the challenge, the more card information is obtained during an intercepted log-in. While longer challenges do increase resistance to brute force attacks, they also decrease usability. Entrust has modeled a variety of different combinations and has found that a challenge length of three cells can provide optimal security –increasing resistance to brute force and intercepted log-ins.

Perhaps even more important than these detailed security considerations is the fact that an organization can help to avoid attacks simply by deploying a solution that makes them less vulnerable and, thus, a less attractive target for attackers.

[4] Comparison with the average number of intercepted logins required to capture the authentication factor.

[5] Entrust's security experts can help customers confirm the configuration best suited to specific customer requirements

5.3 Multi-Channel Authentication

Entrust IdentityGuard can be readily extended for other authentication needs. In many cases, transactions with users are not exclusively performed using Microsoft Windows desktops and the corporate network. Organizations deploy resources and make information available to users from anywhere at anytime via corporate Intranets. Web access to such sensitive information can benefit from the added authentication security offered by the Entrust IdentityGuard solution. Alternate channels may also include the telephone or a mobile device such as Personal Digital Assistant (PDA).

The Entrust IdentityGuard solution can also be leveraged using alternate methods to communicate to third parties such as customers, partners or legislative and regulatory bodies that are outside of the organization. The challenge and response method used with Entrust IdentityGuard does not require the actual display of challenges, nor does it require complex time-based synchronization. For example, an Interactive Voice Response (IVR) system could automatically prompt a user with a coordinate challenge to which the user would key in the response using their touch-tone dial pad.

Thus, by making an investment in this single mechanism, an organization could provide greater security across the numerous ways it communicates with its users, helping to reduce expenses and simplify a user's experience.

6 Easy, Cost Effective Deployment

Regardless of the strength of the security, no mechanism for authentication can be successful if it is costly and complex to deploy. Traditionally, the only choice for an organization that wanted to provide greater protection from on-line identity theft was to employ some form of cryptographic token or complicated scratch pad approach. Entrust IdentityGuard is designed to be cost effective throughout purchase, deployment and on-going management making it a more viable method to authenticate not only permanent employees but also for temporary employees, contractors and partners as well.

6.1 Deployment

Entrust IdentityGuard is inexpensive to produce and deploy. The Entrust IdentityGuard solution is not dependent on the physical factor being used to deploy the user's grid. As a result, organizations can choose the method most cost effective and convenient for them, such as attached to biweekly pay reports which are already distributed to employees or printed on the back of employee identification badges.

The Entrust IdentityGuard solution manages the grid contents for a given user and provides it in an XML data format for integration into the desired fulfillment process, such as the production of an employee identification badge or a simple plastic card as shown above.

In contrast, hardware tokens must be purchased at a significant per user cost and physically distributed. Due to their form factor, their distribution typically requires a stand-alone process, again at significant cost to set up and manage.

Even one-time password approaches such as scratch-pads can have high production and distribution costs. Typically, these consist of a series of one-time passwords, each to be used once during login. To help the user track which one is to be used at a given time, each one-time password is often covered with scratch material similar to that used in lottery tickets. Thus, the user would begin the login process, scratch and uncover the next password to use.

Because of the practical limitation on the number of one-time passwords that can be provided on a single scratch sheet, this authentication method would have to be re-deployed frequently – potentially every few weeks. The scratch feature of the password list combined with the frequency of distribution significantly increases deployment costs and administrator time.

Entrust IdentityGuard supports a variety of use cases for deployment. It is important to accommodate the different mechanisms organizations will use to physically distribute the Entrust IdentityGuard grid allowing users to benefit from immediate access to Microsoft Windows desktops and other on-line services. Example use cases are as follows:

- The simplest case is for users who can physically obtain their cards at the same time they are added as Entrust IdentityGuard users. This allows them to obtain their grid and to use it immediately.
- Users who cannot immediately pick up their grid, but can do so in a reasonably short time frame (ex. within one day) can take advantage of an Entrust IdentityGuard temporary passcode. This allows a passcode to be used for a limited time or number of logins until the user obtains their grid. By being of limited life, the passcode provides a low risk approach to provide users access until they obtain their new grid.
- In some cases, it is necessary to physically distribute grids by mail while still providing immediate access to users. In those cases, a temporary soft-copy grid can be created and distributed electronically and viewed via applications such as Adobe Acrobat. This would be used until a physical grid replacement arrives by mail. To ensure the security of this process, the soft-copy grid would be different and have a limited lifetime.

6.2 Reduce On-Going Management Costs

Lifecycle costs of Entrust IdentityGuard can be reduced using sophisticated management capabilities. On-going management costs can often overshadow actual procurement and deployment expenses. This is largely driven by three key cost factors: ease of use, reissue and user recovery.

If users are not willing or do not find strong authentication easy to use, there is significant potential for help desk calls to drive up support costs. Entrust IdentityGuard's grid challenge and response method makes it a very easy to use authentication method. Further, reducing the need for any specialized hardware increases portability and convenience.

Re-issuance of authentication devices can represent significant on-going costs. However, in contrast to traditional hardware tokens, issuing a new Entrust IdentityGuard grid can be very inexpensive due to its low production and fulfillment cost. It also is simpler than the scratch-pad approach which requires each user's password list to be monitored and replaced in sufficient time to make sure the end user doesn't run out of passwords.

It is inevitable that replacement second factor devices will be required if the second factor is lost or forgotten. It is very important that these situations do not result in significant help desk expense or with the user being prevented from performing transactions for extended periods of time. Not only can this increase costs, but it can also negatively impact the user's perception of the organization. To help prevent this, the Entrust IdentityGuard solution provides the temporary passcode mechanism described previously.

The temporary passcode can be provided virtually immediately to the user should they lose or misplace their card. Likewise, where it will take some time to distribute the replacement Entrust IdentityGuard grid, a temporary soft-copy grid can be used for greater security until the permanent replacement arrives. Entrust IdentityGuard Client for the Microsoft Windows platform supports the use of the temporary passcode both

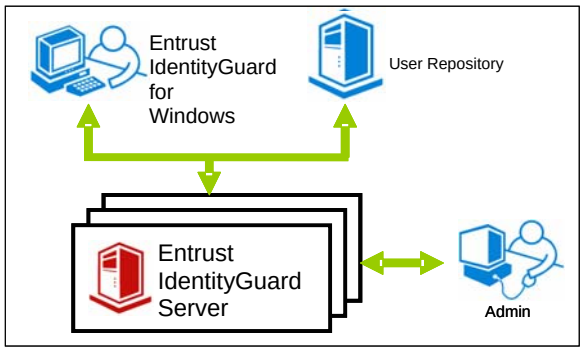
online when a user is connected to the corporate network and offline when no connection exists to ensure that authentication security is always maintained. For example, if a user misplaces his grid while on the road, or forgets the grid at home or the office, a temporary passcode will give them access to their desktop even if they cannot connect to the corporate network.

All of these mechanisms can help to enhance the security provided by Entrust IdentityGuard and more cost effectively meet an organization's requirements for stronger authentication.

7 Architecture and Integration

Entrust IdentityGuard solution has been designed to work in an organization's environment with minimal impact to existing infrastructure and desktops. IdentityGuard Client for the Microsoft Windows platform does not replace the Windows authentication interface. It simply adds an extra step to the authentication process by which Microsoft Windows desktop users can be asked to respond to an IdentityGuard challenge before getting access to the desktop and consequently to the corporate network. Without completing both the Microsoft Windows and IdentityGuard authentication operations, users cannot have access to their desktop, nor can they access the corporate network directly, over a wireless network, or over the Internet through a VPN.

Entrust IdentityGuard has also been designed to help accommodate the high scalability needs of consumer applications, providing the availability and service levels required in that type environment.



7.1 Low-Impact Integration

Entrust IdentityGuard Client for Windows is designed to compliment an organization's current Windows desktop environment.

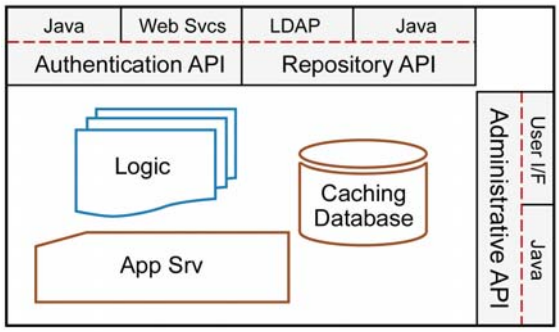
Entrust IdentityGuard Client for the Microsoft Windows platform is a small footprint client that provides the Entrust IdentityGuard challenged as a second step to Windows authentication. It is deployed and installed on user desktops using Windows Installer technology and has achieved the Designed for Windows XP logo certification.

Entrust IdentityGuard leverages the customer's existing repository. This repository, such as Active Directory, is leveraged to store and retrieve the card data for a given user. When a card is generated for a given user, it is stored in encrypted form in the repository. When a user is being authenticated, it is retrieved from the repository.

Finally, a secure remote Web interface is provided to access the various user and card management functions. This includes the ability to create new cards, assign temporary passcodes and update user and card status. Administrative functions are also available via API to make them available to user identity management and provisioning systems.

7.2 Robust, Flexible Architecture

The Entrust IdentityGuard server has been designed to meet the scalability requirements of the largest organizations. As such it is designed to accommodate several servers deployed at one time in a load balanced environment. This allows for increased throughput by adding additional servers. Also, an embedded database is provided to cache user and card information to accelerate transactions.



The Entrust IdentityGuard solution leverages the Entrust IdentityGuard server installed in the organization's current infrastructure. It is written in Java and runs on the Linux operating system. Security operations including generating, encrypting and decrypting card contents are performed using Entrust's FIPS 140-2 and Common Criteria certified cryptographic software. Use of these standards helps to protect the content of each card, reducing the risk of a rogue employee (or attacker??) successfully tampering with card information stored in the repository.

Finally, like all Entrust products, software development, quality and security assurance is performed to meet stringent standards. Further, support for the Entrust IdentityGuard solution is available and provided by Entrust's global service and support organization.

8 Summary

As the threat of unauthorized access to corporate desktops and networks continues to grow, organizations will need to proactively mitigate the risk with a stronger form of authentication that is easy to use and less costly to purchase and deploy. Entrust IdentityGuard solution can help address this need by providing a simpler, innovative and inexpensive way of increasing security and defending against attacks. Any organization looking for a second factor of authentication that is simple and inexpensive should consider piloting Entrust IdentityGuard.

Entrust IdentityGuard is part of the Entrust Secure Identity Management solution and is integrated into the other strong authentication and access control elements of the Secure Identity Management solution. For more information on how Entrust IdentityGuard can help you improve user authentication to desktops and networks, please visit: **http://www.entrust.com/IdentityGuard/.**

9 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities.