

**Protecting Our Data:
The Next Step to Improve Security
in the Real Estate Industry**

August 1, 2004



**Clareity Consulting & Communications, Inc.
Scottsdale, AZ
(480) 368-8100
<http://www.callclareity.com>**

Introduction

MLS data is the core asset of the real estate industry, and it is crucial that it be protected. An increasing number of MLSs and real estate companies have asked Clareity to research online system access control and data protection methods in order to come up with security solutions that are more reliable than the current username-password mechanism. Unauthorized system access and theft of data has become a national epidemic due to lax password-only security.

Over the past two years, Clareity has performed significant research on data protection and user authentication (system access control). We first presented “strong authentication” as an important security component for MLSs to consider implementing during our presentation at the Council of MLS meeting in 2002 and at subsequent Clareity Workshops. We believe it is now time for the industry to take action to improve its lenient security practices.

To quote Bob Butters, Partner with the law firm of Arnstein & Lehr, Chicago, IL (formerly Deputy General Counsel at NAR and a lawyer with the FTC):

"Unauthorized use of Participant access codes can lead to MLS liability and loss of MLS' valuable proprietary rights. Not only can the economic value of the MLS' database compilation be undermined, but non-public showing instructions falling into the wrong hands can lead to MLS liability for personal injury and property damage."

The following pages:

- Explore the security issue facing real estate web site and MLS operators
- Explain “strong authentication” and how it solves the current issue
- Present the most viable and practical authentication solution

The Current Security Issue

The simplest and most common form of authentication (the process of verifying the identity of an individual) used in IT today is user login name and password. However, there is a fundamental flaw with this method of authentication: there is no guarantee that the *user* of the password is the *owner* of the password.

According to a poll conducted by the Human Firewall Council (now known as the “Information Systems Security Association”):

- 52% of office workers polled would download company information if asked to by a friend
- 42% would tell a friend their password
- 64% already gave their password to a colleague
- 2 out of 3 gave their company password to the pollster!



A separate survey conducted in April 2004 by the organizers of the Infosecurity Europe conference found 71% of office workers were willing to part with their password for a chocolate bar. (Yes, a chocolate bar.) Some 37% of the workers in that survey immediately gave their password to the pollster, and prompting questions raised that number substantially. There is no reason to believe that the real estate industry protects its passwords any better.

As long as there has been an electronic MLS, agents and brokers have shared their MLS passwords. Clareity has found MLS members sharing their login information with technology vendors, friends and family, and even the consumer. With the advent of easy-to-use web-based systems, password sharing has become even more widespread. Whether these passwords are used by “harmless” non-member users, such as part-time Realtors who are not paying for MLS service, or unauthorized data pirates, the simple truth is that MLSs are no longer members-only systems. *MLS system passwords – and access – are simply out of control nationwide.*

Recent postings to MLS e-mail groups confirm the real estate industry is in need of a solution to stop the illegal access and distribution of MLS data. Andy Duplay, MLS Director of the Toledo Board of Realtors, asked, “How do we ... not let others ‘capitalize’ on this and share ID and password among licensed staff in their office, to avoid paying MLS dues?”

To quote Carl DeMusz, President and CEO of Northern Ohio Regional MLS (NORMLS):

"We have ... stiff fines for sharing user names and passwords. That does not mean we can now sit back and not police it ... You can't be weak on your enforcement if you want to control the data and keep it from falling into the wrong hands."

"I think we need to remember that the MLS has been given protective custody of the listing broker's listings. I see many MLS's these days taking that for granted ... If we as MLS's can't prove to be trusted with the listing broker's listings there can be retaliation and there could be a price to pay for not getting our house in order."

John Mosey, President of Regional MLS of Minnesota, said:

"Most of us are blissfully, and in most respects, willfully, unaware of what is happening to the data. We jump all over any cases of misuse or piracy that come to our attention, but I believe what we don't know is where the true threat to our rights of ownership will be found. It is most certainly the duty and responsibility of MLS Executives to be constantly on guard regarding the security of our systems and data."

Controlling access to the MLS – and to transaction management systems, broker systems, and other real estate information systems – is now more critical than ever, since it is no longer just listing information at stake. MLS systems now include a host of contact management and CRM applications that store personal information about clients and prospects. With transaction management system adoption on the rise, access to the



MLS system now provides entrée to a whole new world of sensitive property and personal financial information. While these systems have not yet been subjected to scrutiny under the FTC's Gramm-Leach-Bliley Act Standards for Safeguarding Customer Information, Clarity believes that higher security standards are only a matter of time, given the expansion of sensitive data stored in MLS and transaction management systems.

Password secrecy is now, more than ever, subject to the frailties of human nature:

- Forgetting passwords
- Writing passwords down
- Sharing passwords
- Using a common password for all their accesses
- Stolen passwords

User techniques for avoiding password security obviously negate the intent and purpose of the password. Therefore, reliance on this form of login authentication has caused MLS access to become inadequately controlled. It is only a matter of time before there is an embarrassing and damaging public incident involving a breach of privacy on an MLS system.

In order to deal with the inherent weaknesses in password-based login authentication, which both protects MLS dues revenue and provides a proper level of protection for listing, consumer and financial information, Clarity recommends that MLSs implement "strong authentication."

Strong Authentication Solves the Password Problem

There are three factors of authentication: 1) something you know, for example, a password; 2) something you have, for example, a smart card or other token; and 3) something unique about you, such as a fingerprint.

That third item, "something about you," is commonly referred to as "biometrics." Biometrics eliminates the problems associated with password management by measuring human characteristics such as voiceprint, fingerprint, iris pattern, and facial contours, which are virtually impossible to duplicate and cannot be lost like traditional passwords. While biometrics can be a very powerful tool, Clarity does not recommend it for MLS or other real estate systems because of the high implementation and support costs, especially in our industry's distributed and mobile work environment. Therefore, Clarity focused its strong authentication research on combining "something you have" with "something you know."

A common example of this type of strong authentication is your ATM or bank card. Such cards are called 'tokens' in IT security parlance. Tokens require something you have (your card), and something you know (your PIN). You wouldn't want your bank to allow access to your account with just one of these factors - the risks are far too great. Yet in the real estate industry, sensitive data can be accessed with just one factor - a weak,



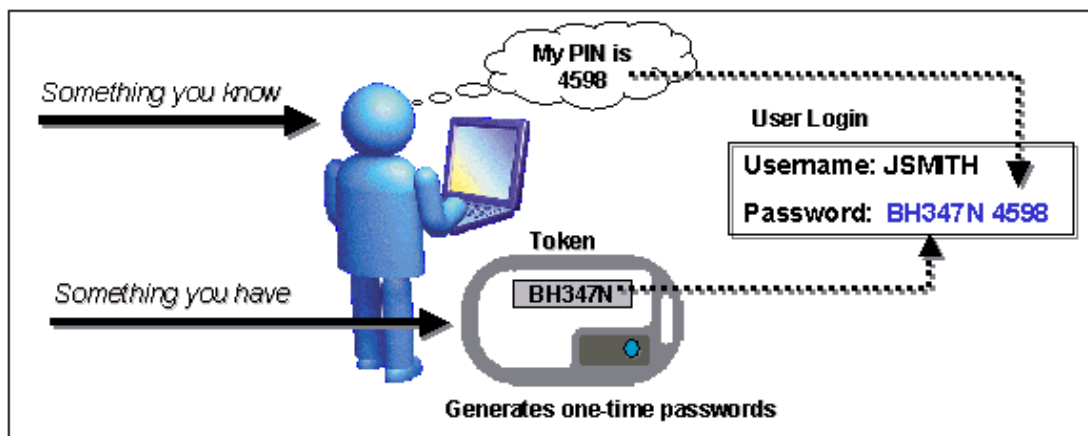
memorized password! Strong authentication eliminates password risks by providing *multi-factor* authentication. Best of all, strong authentication is not new behavior for humans, as we can all relate to the ATM card example.

“Something you have” can take several forms, but is generally classified as follows:

- A physical smart card or USB token
- A ‘digital certificate’ / software token

The best form of these tokens generates a dynamic, one-time pass code that the user enters to access the system. Most of the vulnerabilities of memorized passwords (sniffing, guessing, hacking, sharing etc.) are eliminated if the user requires a different password each time they log into the system, as any pass code obtained or given to a non-member user would be outdated as soon as it was used.

Dynamic, one-time-passwords work like this:



Instead of entering a username and password into their login screens, users type in their user name, push the token button (and possibly a PIN code for extra security), and enter the pass code that the token displays. It's simple, fast and painless. Once a pass code is used, it can't be used to log in again.

There are hundreds of companies offering various types of strong authentication products today. Clarity spent significant time researching and identifying which company could provide the right solution for the real estate industry.

About Secure Computing

Clarity selected Secure Computing as the leading candidate for providing an MLS strong authentication solution based on several factors:

- 1) The company's proven track record and company stability
- 2) The full range of the security solution offering
- 3) 24 x 7 x 365 staff support



- 4) History of innovation
- 5) Ease of integration with other systems
- 6) Competitive pricing

The company and its strong authentication product are extremely well regarded in the security industry. In 2002, *SC Magazine* rated it the Best Buy and gave SafeWord PremierAccess five stars out of five in every category (features, ease of use, performance, documentation, support, value for money). According to *SC Magazine*, the product offers "Great choices, strong security, extremely scaleable and ease of manageability exceeded expectations."

To quote Frank Gillman, Director of Technology at the large law firm of *Allen, Matkins, Leck, Gamble and Mallory LLP*, "I wish every technology we deployed was this successful. PremierAccess worked right out of the box."

Secure Computing is also eager to work with Clarity to tailor its security products and services for MLS and the real estate industry - and that process has already begun.

Track Record and Stability

Secure Computing (NASDAQ: SCUR) has been securing the connections between people and information for over 20 years. Specializing in delivering solutions that secure these connections, Secure Computing is qualified to be a security solutions provider to organizations of all sizes. The company has over 11,000 global customers, including the majority of the Dow Jones Global 50 Titans and the most prominent organizations in banking, financial services, healthcare, telecommunications, manufacturing, public utilities, and government. Secure Computing has close relationships with the largest agencies of the United States government, including multiple contracts for advanced security research.

SafeWord PremierAccess customers include hundreds of leading firms in banking, finance, government, and various high-tech industries, totaling over three million end users. Deployments range from very small companies and government organizations to one of the world's largest aircraft manufacturers with 100,000 users and one the world's largest banks with 800,000 users. There is no question that the SafeWord PremierAccess solution can scale to meet the needs of even the largest MLS.

Secure Computing is consistently rated to perform at or above the rest of the market segment, and revenues for this profitable and growing company have more than doubled in the past four years:

Year	2000	2001	2002	2003
Revenues	\$34.64M	\$48.35M	\$61.96M	\$76.21M

Secure Computing is headquartered in San Jose, California. (For more information on the company, see <http://www.securecomputing.com>.)



Full Range of Solutions

Secure Computing's SafeWord PremierAccess solution provides many authentication options, including passcode-generating tokens, digital certificates, smart cards, biometrics, and text-messages to wireless devices such as cell phones, pagers and Palm Pilots. An MLS can mix and match any or all of these solutions to offer the best, most flexible solution for all of its members.

Some of the forms of Secure Computing's SafeWord PremierAccess Tokens



Silver 2000



MobilePass
(For cell phone / Palm Pilot)



Gold 3000



Smartcard



Platinum



iKey 2000

Clareity believes that a combination of any of the following three forms of strong authentication will make the most sense for the real estate industry:

Silver 2000

In a convenient keyfob package, Silver 2000 authenticator tokens generate one-time passwords with the simple touch of a button. These passwords, like those generated by the Platinum or Gold 3000 tokens, can be used once, ensuring secure access. No PIN is required to activate this authenticator, although MLS customers may wish to take advantage of the SoftPIN feature, which allows the addition of a PIN entry with the token-generated password providing two-factor authentication.

MobilePass™

MobilePass transmits one-time passwords as text-messages directly to most wireless phones, pagers, or PDAs. This zero-footprint solution provides the security of a token without requiring any other hardware or client software - MobilePass works with the devices users already have. MobilePass sends one-time passwords to the user's cell phone, pager, or wireless PDA.

SofToken™ II

Secure Computing's software-based token, SofToken II, is for users who want the security of one-time passwords but do not want to carry a hardware token. SofToken II generates a dynamic password just as the handheld tokens do, but the SofToken II software resides on the hard drive of the user's laptop or desktop system.

24 Hour Support

Secure Computing provides 24x7x365 staff support. Clareity will help your organization through the process of integration, and provide staff training and on-site assistance during implementation. Optionally, Clareity can also provide end-user training during the deployment.

Clareity will also function as a front-line account representative for staff and on-call troubleshooting partner with Secure Computing.



Comparison with the Competition

In May 2004, Secure Computing's strong authentication solution was awarded the Editor's Choice and the only "A" rating by Network Computing's Secure Enterprise Magazine in a head-to-head comparison with other market-leading authentication products. Those products included ActivCard's ActivCard Token, RSA Security's RSA SecurID, and Vasco's Vacman Middleware and Controller.

Further comparing the Secure Computing solution with its competition:

- The US Department of Justice performed tests on both Secure Computing tokens and those of a major competitor – including washing machine, freezer and oven tests. Secure Computing tokens had a 95% *survival* rate while the competitor's tokens had a 95% *failure* rate
- Secure Computing has the simplest integrations, as documented in all of the magazine articles quoted above.
- Secure Computing has the only automated deployment and self-enrollment mechanisms
- Secure Computing does not charge for failover servers, while the competitors (at least those that support such important functionality) charge extra.
- Secure Computing does not charge extra for 24x7x365 support

Secure Computing's competitors simply do not offer the variety and quality of products, and while some of them sell cheaper authentication tokens, their extra costs add up.

Secure Computing's solutions offer world-class authentication security and Clarity estimates the total cost of implementation, including 24 x 7 technical support, to be in the \$1.50 to \$3.50 per member per month range, depending on the security solution and financing options selected by the MLS.

According to Eric Hemmendinger, Research Director, Security and Privacy of the *Aberdeen Group*, "Fitting together authentication and access control solutions from different suppliers is an integration nightmare that is usually handed off to high-priced consultants. With the introduction of SafeWord PremierAccess, Secure Computing is delivering pre-integrated solutions for access control and user authentication that are plug-compatible with existing applications. The result for IT buyers is less time and money spent on integration, and a better fit between the old and the new security solutions."

When *Security Pipeline* tested a number of competitors in the strong authentication space, including Secure Computing's SafeWord PremierAccess, ActivCard's ActivCard Token, RSA Security's RSA SecurID, and Vasco's Vacman Middleware and Controller, the PremierAccess product came out on top again:

"So who wins? Secure Computing's SafeWord PremierAccess offers one of the easiest ways to build AD-linked hardware authentication into your security plan. It's our overall winner because its schema modifications are performed according



to Microsoft standards and its plug-in approach to integration makes tying it to AD easy.”

Clareity is confident that Secure Computing is the best company to provide strong authentication to the real estate industry.

Clareity and Secure Computing

After considering the aforementioned test results and rigorously comparing available solutions, Clareity has become Secure Computing’s vertical market partner for the real estate industry. Clareity will be working to help Secure Computing tailor its world-class security technologies to provide powerful and practical products for real estate. The customized solutions will provide security across a broad spectrum of real estate IT systems and will be specifically designed for mobile professionals. They will provide MLSs and real estate companies with heightened security while being easy to use and inexpensive.

Clareity will help your organization through the process of tailoring and implementing the right security solution for your MLS. This includes planning the installation with your vendor or staff, system integration, staff training, and providing on-site assistance to guarantee the success of your deployment. Clareity supports Secure Computing products and functions long-term as the company’s front-line account representative for staff and as its troubleshooting partner. Clareity’s ongoing relationship with Secure Computing will help ensure your organization receives the highest level of service over the life of your contract. Clareity can also coordinate cooperation and compatibility in markets where there are multiple or neighboring MLSs implementing Secure Computing’s products.

See a joint Clareity and Secure Computing Presentation:
A Secure Computing executive will be joining Matt Cohen, Clareity’s Chief Technologist and security guru on the stage at the Inman Connect Conference (<http://www.inman.com>) on Thursday, July 29th at 4:15pm for a joint presentation on Security and Strong Authentication. We hope to see you there!

Gregg Larson
Matt Cohen
Matt Cobo
Kevin Hughes
Marie-Anne Varga

For more information, or to request a proposal or pricing for Secure Computing products, please contact:

Kevin Hughes
Clareity Consulting
Kansas City, Kansas
(913) 248-8604
kevin.hughes@callclareity.com

Gregg Larson
Clareity Consulting
Scottsdale, Arizona
(480) 368-8100 x201
gregg.larson@callclareity.com



Technical Specifications and MLS System Integration

Ease of Product Integration

Secure Computing has already developed integration methods that bypass the usual nightmare of application integrations that have plagued other authentication solutions. The following integration methods will make it easy and economical to integrate the Secure Computing solution with applications used by the MLS and others in the real estate industry:

Universal Web Agent and Web Login Server

Many organizations providing extranet access or web content have a range of different web servers, such as IIS, iPlanet, Apache or custom application servers. Most access control solutions rely on agents or plug-ins that install on the Web server software, which are limited to specific Web server software or versions. PremierAccess solves these problems with the Universal Web Agent. While most agents protect a specific program, the Universal Web Agent protects the entire operating system that the Web Server operates on.

The Universal Web Agent protects both Windows 2000 and Solaris 7&8 servers. PremierAccess also includes a Web Login Server (WLS) that works in conjunction with the UWA. The WLS is an independent Web server that you can install on the same box, or on a separate box from the UWA. The WLS intercepts Web traffic, requests authentication, and verifies user identity with the PremierAccess AAA (authentication, authorization, administration) server. Once a user is authenticated, a session cookie is created with a session ID number and role-based authorization information. These credentials are passed to the UWA, which enforces what pages or Web resources the user can access.

SafeWord PremierAccess support for VPNs

SafeWord PremierAccess adds critical strong authentication to positively identify a user before an encrypted VPN tunnel is established--an essential component of any secure VPN solution. Secure Computing offers robust and scalable solutions that work with all major VPN vendors including Cisco (Concentrator 5000 and Altiga 3000), Check Point (VPN-1/FireWall-1), Microsoft Windows 2000, Nortel (Contivity), and Alcatel (7130 Secure VPN).

SafeWord Agent for Windows Domain

The SafeWord Agent for Windows Domains is a Windows domain login module that lets companies provide secure access to NT and 2000 domain-based networks.



Additional Integrations

Secure Computing provides integration modules for Citrix®, TACACS+, NT remote access server (RAS), Novell Modular Authentication Service (NMAS), Pluggable Authentication Modules (PAM) and SID2.

Software Development Kit (SDK)

Going even further, Secure Computing, published the PremierAccess SDK (software development kit), designed to enable developers to add SafeWord authentication to their own applications. The SDK contains code, documentation, strategies for building configurations, and sample programs that demonstrate how to use the API. The SafeWord Authentication SDK provides several advantages to developers. It includes a facility for authenticating passwords using SafeWord technology. The SDK allows programmers to easily add SafeWord capability to their applications and is ideally suited to both new development and retrofits. SafeWord's SDK integrates into applications developed for Microsoft NT, Solaris/SPARC, Linux, and other operating environments.

About Clareity

Founded in 1996, Clareity continually provides its clients truly independent and unique perspectives and insights. Clareity has successfully executed a vast array of consulting projects for our clients, related to:

- IT Security Audits and Assessments
- Creation and analysis of RFPs for MLS systems, public records, broker systems, and transaction management systems
- Product integration specifications
- Competitive analysis
- Contract negotiations
- Project management and implementation assistance
- Mergers, acquisitions and strategic alliances
- New product marketing and business plans
- Recruiting and staffing services
- Expert witness and opinions
- Market research including electronic surveys, interviews, and focus groups
- Strategic Planning

For more information please contact:

Gregg Larson
Clareity Consulting and Communications, Inc.
Scottsdale, Arizona
(480) 368-8100 x201
gregg.larson@callclareity.com
www.callclareity.com



Copyright © 2004, All Rights Reserved
Clareity Consulting and Communications, Inc.
Scottsdale – Minneapolis – San Francisco – Kansas City
www.callclareity.com