Stratecast A Division of FROST & SULLIVAN

Effective and Painless Multi-Factor Authentication

February 2011

www.frost.com

EFFECTIVE AND PAINLESS MULTI-FACTOR AUTHENTICATION

There is a new, multi-factor authentication approach that not only strengthens identity authentication but does so in a way that does not introduce the burdensome cost, user inconvenience, and administrative complexity that have limited the adoption of multi-factor authentication by small and mid-sized businesses.

INTRODUCTION

When the information age was young, authenticating user identity with a high level of confidence was simple—assign the user a password. For the majority of computer system users, this was the only password each had and the password could only be used in one place—at a stationary workstation within the physical confines of his/her place of employment. Being a credentialed user also had status; the user was now a member of a privileged group. Consequently, user acceptance of the 'given' password, no matter its complexity, was high. These privileged users would devote the necessary time to commit the password to memory. For system administrators, this combination of memory-intensive passwords, confined user populations, and a computer system that was accessible only through dedicated and observable workstations amounted to user authentication with limited risk of compromise.

This is so ancient; the world today no longer resembles this picket fence scenario. User populations have expanded exponentially and users access numerous distinct systems in their work and personal lives with each system requiring credentials—typically a username and password. Coping with an onslaught of system credentials, it is no surprise that users have reverted to tactics that invalidate the intended security strength of passwords: relying on easy to remember password conventions, using the same password across many systems, changing passwords only when absolutely necessary, and even writing down their passwords. Furthermore, system access is no longer bound to a location or dedicated workstation. Thanks to the Internet's reach, users access systems from anywhere with any browser-enabled device. Line of sight observation of who is requesting system access doesn't exist. The Internet has also given way to a higher risk of identity theft via phishing schemes and keyboard logging malware.

Yet, even with the slide in the security strength of passwords, the use of passwords as the only means to certify a user's identity still remains prevalent among small and mid-sized businesses (SMBs). This risky practice, however, does not need to be. There is a new, multi-factor authentication approach that not only strengthens identity authentication but does so in a way that does not introduce the burdensome cost, user inconvenience, and administrative complexity that have limited the adoption of multi-factor authentication by small and mid-sized businesses.

In this white paper, we describe why multi-factor authentication is rising in importance, briefly review the pros and cons of different multi-factor authentication approaches, and end with an introduction and assessment of RSA® Authentication Manager Express.

WHAT IS MULTI-FACTOR AUTHENTICATION—AND WHAT ARE FACTORS?

The objective of identity authentication is to establish a bond of trust between an organization and the user who is requesting system access. More specifically, identity authentication ascertains a level of trust regarding who the user claims to be. It follows that the more pieces of evidence, that is authentication factors, the user can present to prove his/her identity, the stronger this bond of trust becomes. Similarly, the more irrefutable the factors are, the bond of trust is also strengthened.

Authentication Factors

There are several types of authentication factors. The most common type is ***something the user knows***, such as a password. Passwords, however, are not totally irrefutable forms of authentication. For example, short passwords, passwords embedded with guessable phrases, and static passwords contribute to passwords being compromised.

Another authentication factor is ***something the user has***, that is, proof by possession. Essentially, the user possesses something that is unique. That possession could be a USB token. A one-time password (OTP) key fob, or a cell phone, can also be something that the user has. With these, the user enters a one-time password received on the key fob, or an authorization code sent via SMS messaging to the user's cell phone, as part of the authentication process. As long as the possession of the USB token, OTP key fob, or the user's cell phone remains with the user, possession-based factors demonstrate strong evidence of the user's identity.

Something the user is is another authentication factor. A common application of this factor is picture IDs, for example, as used at airport terminal check points. Does the picture on the ID card resemble the cardholder? While practical for airport terminals and other gateways that accommodate human-to-human interaction, the same is not true for computer system access where the factor checking is typically a human-to-machine interaction. For system access, biometric scans, such as through a fingerprint reader, compare a scanned fingertip to an archived image. As each fingerprint and other forms of biometrics are unique, this type of authentication factor, with a reliable scan and comparison to the archived image, is also a strong factor.

Rounding out the range of authentication factors is ***something the user does or how the user behaves.*** With this authentication factor, current user behaviors are compared to a historical behavior profile of that user. If the current behaviors are consistent with the established profile, this evidence supports user authenticity. Conversely, if there is a profile deviation, this raises doubt that the user is who he/she claims to be. ATM, debit, and credit cards exemplify a simplified application of behavioral-based authentication. For example, if card use does not adhere to an established profile (e.g., a spike in transaction frequency), transaction process could be suspended due to concern that the card is no longer in the possession of the registered cardholder. A relevant example with computer access is location (e.g., as defined by IP address), where the user is originating access from a different location than is customary.

No authentication factor is absolutely irrefutable in its association with the user. With sufficient effort, intelligence and creativity, each can be compromised. Additionally, the strength of some authentication factors—for example, something you know—is dependent on the user. If a user doesn't protect his/her identity-confirming factor, a bond of trust based solely on an "unprotected" factor is inherently weak. Fortunately, different forms of authentication factors are not related to each other, such that weakness in one authentication factor does not automatically point to similar weakness in other factors. For this reason, authentication based on two or more independent factors reinforces the bond of trust between the organization and access-requesting user; the collective power of many creates stronger authentication.

No authentication factor is absolutely irrefutable in its association with the user. With sufficient effort, intelligence and creativity, each can be compromised.

♦♦♦

Authentication based on two or more independent factors reinforces the bond of trust between the organization and access-requesting user; the collective power of many creates stronger authentication.

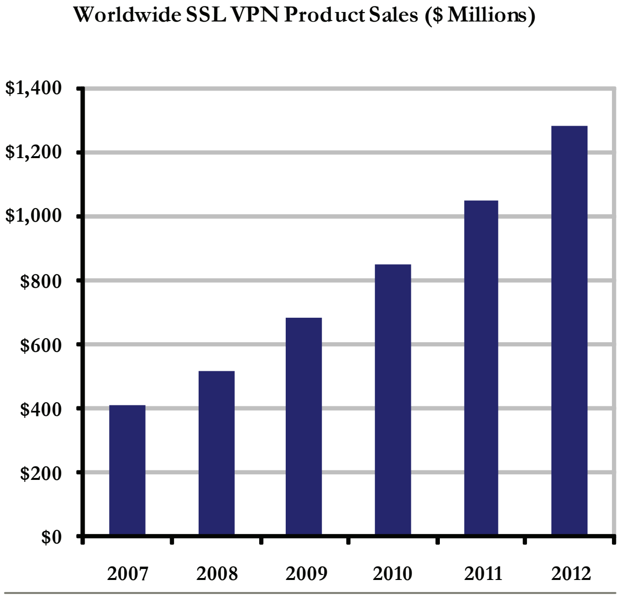
THE RISING NEED FOR MULTI-FACTOR AUTHENTICATION

There are several reasons why SMBs are, and should be, taking greater interest in multi-factor authentication. In this section, we highlight three prominent reasons.

Passwords as the only authentication factor are inherently weak – Several reasons were previously stated that point to the growing weaknesses in passwords as strong authentication factors. One reason that stands out is user responsibility. All of passwords' security weaknesses, to some degree, are tied to what the user community will tolerate. Unless all users in the business organization accept the responsibility to use and protect complex passwords and change them regularly, there is greater risk of a security incident. But is this risk growing? That depends on the value of the information that system access permits. If the value of the information is increasing but password security policies and user compliance are static or sliding into leniency, the risk of an information breach, and the resulting impact on the business organization, is also increasing.

Physical proximity between users and computer systems is blurring – The pervasive reach of the Internet and its broadband speeds have made remote access to computer systems not just feasible for nearly everyone, but demanded. For employees, remote access supports their flexibility in fulfilling more of their work activities without the constraint of being office-bound. For business owners, remote access is not just good for its employees, it's good for business. Employee remote access boosts productivity and improves a business' agility in responding to customer needs and in adapting to competitive forces. Furthermore, remote access to computer systems is not limited to employees but increasingly includes a diverse user community consisting of business partners, customers, and temporary workers. Also, it is worth noting that in this intensifying information age, information is currency. If information cannot be fluidly exchanged among legitimate users, businesses will find themselves at a competitive disadvantage. Even so, remote access users are virtual users and, as such, the ability to confirm a user's identity through observation, as in an office-bound scenario, doesn't exist. Multi-factor authentication is a crucial mechanism in protecting computer systems and their vast stores of information from intruders and imposters.

Indicative of this rise in remote access is the steady increase in sales of SSL VPN gateways, as shown in this chart. With these gateways, businesses can establish private connections through the Internet between remote access users and their internal systems. Moreover, SSL VPN connections can be made, regardless of users' device type (handheld, tablet, laptop, and desktop) and device ownership (user-owned, business-owned, and shared). This attribute of SSL VPNs has been particularly popular with businesses that need, or are compelled by their user communities, to permit remote access from an ever-widening array of browser-enabled devices.



Remote access users are virtual users and, as such, the ability to confirm a user's identity through observation, as in an office-bound scenario, doesn't exist.

Stiffening Information Privacy Regulations – From our perspective, there are three themes to note with regard to information privacy regulations: (1) regulations are established long after information breaches have occurred, (2) there will always be an element of subjectivity on how to be compliant, and (3) substantiating compliance is a cost of doing business. From these themes, we have reached the following conclusions.

- ***Waiting for regulations to materialize before taking steps to reduce the risk of information breaches is unwise.*** Individuals that are impacted by an information breach will not be appeased by the excuse that "we were not formally obligated to take steps or explicitly instructed on how to protect your sensitive information". The damage done can have a very long recovery cycle.
- ***Being "amply" compliant is better than being "marginally" compliant.*** Why? The threat landscape is continuously evolving, and regulations and/or the accepted interpretation of what constitutes being compliant will evolve, too. Therefore, an extra ounce of prevention taken now to exceed compliance could be more economical and less disruptive than having to revamp business operations and security practices in the future. Additionally, the time and cost to substantiate compliance may also be reduced by following an amply compliant path.
- ***Multi-factor authentication is no longer just a "best security practice"; it's a "smart business practice".*** Migration from single-factor authentication to multi-factor authentication will not only reduce information security risk but it can also reduce direct and indirect regulatory compliance costs. Still, few business decisions, even the most obvious ones, do not follow a one-size-fits-all

solution approach. There are options in multi-factor authentication that should be weighed before making the move.

CHOOSING A MULTI-FACTOR AUTHENTICATION SOLUTION

Previously in this paper, we briefly described four types of identity authentication factors:

- Something the user knows
- Something the user has
- Something the user is
- How the user behaves

We also noted that there is strength in numbers; the more independent authentication factors that the user presents for identification, the stronger the authentication or bond of trust. This is true up to a point. A password as simple as "12345" has virtually no authentication strength. It is easily guessed and, even if combined with another authentication factor, the two do not, in practical terms, constitute multi-factor authentication. Therefore, the degree of irrefutability—that is, how strongly associated a factor is with the factor-presenting user—comes into play. This is true not just in comparison of different types of authentication factors but within the same type. For example, an eight-character password consisting of letters, numbers, and special characters will have a stronger association with the presenting user than the simple 12345 password. Strength in multi-factor authentication is not only dependent on how many factors, but which ones and the association strength of each with the authenticating user.

Strength in multi-factor authentication is not only dependent on how many factors, but which ones and the association strength of each with the authenticating user.

♦♦♦

A multi-factor authentication solution that can support several authentication factors, and a variety of combinations of those factors, is superior to a solution that is more limited.

With a perspective on leveraging multi-factor authentication effectively, we recommend that as SMB security decision-makers evaluate multi-factor authentication solutions, they consider the following attributes.

- **Flexibility** – In military and intelligence agencies, information is classified based on its sensitivity. For example, top secret classification is assigned to the most sensitive information and, correspondingly, requires the highest level of trust in the user's identity before access to this information is granted. At lower classification levels—secret, confidential, and then unclassified—the required level of trust is dialed down, as the risk to national security due to an information leak is less. Although the typical small or mid-sized business is not in possession of information pertaining to national security, it still has information, computing systems, and software applications of varying sensitivity. For this reason, a multi-factor authentication solution that can support several authentication factors, and a variety of combinations of those factors, is superior to a solution that is more limited. Matching authentication strength with risk, or the protection needed, follows the core principles of effective risk management.

- **Cost** – Typically the cost of authentication is correlated with investments in hardware components. The more hardware required, the greater the cost. However, hardware-based authentication factors also yield a high degree of irrefutability. For example, producing a counterfeit digital certificate sealed in an encrypted USB flash drive is nearly impossible. Nevertheless, the cost to purchase, distribute, and manage USB tokens, OTP key fobs, and biometric scanners can be more than the cost to set up and administer other types of authentication that are based primarily on software (e.g., password administration and behavior profiling).

- **User Convenience** – Users' actions are driven by their priorities, which do not necessarily correspond to those of the business. The need to control system access is not a user priority; it is, however, for business owners, shareholders, and those tasked with information security. Users want to zoom through identity authentication with as little involvement as possible in order to get to the systems and information that assist them in accomplishing their "get things done" objectives. Speed and transparency are important to users. It comes as no surprise that the aforementioned weakening of password security (e.g., through the use of short and easy to remember passwords) exists today. Another point is that the user community is not just employees but, in many cases, includes guests, such as business partners and customers. For these groups of users, it is particularly important to make their authentication process as streamlined or 'guest-like' as possible.

Users want to zoom through identity authentication with as little involvement as possible in order to get to the systems and information that assist them in accomplishing their "get things done" objectives.

- **Administrative Ease** – Related to cost as an attribute in choosing an authentication solution is administrative ease. Administrators tasked with setting up and managing an authentication process is a cost to the business. The more time spent, the less time administrators have available for other business activities. Moreover, if the complexity of administration requires specialized knowledge or training, the business will incur the premium fee of specialists or risk the consequences of mismanaged strong authentication, if administration is assigned to a less qualified individual. Therefore, administrative ease is crucial in completing administration accurately, time efficiently, and for an acceptable cost. At the front end, businesses are wise to consider the interoperability of the strong authentication solution within their existing network and security infrastructure. A 'work around' installation of the authentication solution will surely add to administrative effort and potential delays when strong authentication becomes operational.

Administrative ease is crucial in completing administration accurately, time efficiently, and for an acceptable cost.

INTRODUCTION OF RSA AUTHENTICATION MANAGER EXPRESS

RSA Authentication Manager Express is a new, centralized authentication platform tailored for small and mid-sized businesses that need to elevate users' authentication strength. Deployed at the edge of a business' network, RSA Authentication Manager Express utilizes tokenless technologies to perform strong authentication on web-based access by employees, business partners, and customers to behind-the-firewall resources.

Core elements designed into RSA Authentication Manager Express are adaptability, affordability, and user- and administrator-friendliness. The four authentication solution attributes from the previous section will be used in the table below to demonstrate how these elements are present in RSA Authentication Manager Express.

Core elements designed into RSA Authentication Manager Express

Attribute	Demonstrtation
Flexibility	Flexibility is demonstrated in RSA Authentication Manager Express' out-of-the-box support of three authentication factors: ▪ ***Something the user knows*** – Password and, as needed, answers to challenge questions ▪ ***Something the user has*** – An identifiable access device and, as needed, a cell phone ▪ ***Something the user does*** – In-depth behavioral analysis based on user patterns, location (e.g., IP address), and past authentication and account activity are used to assess and score the user's authenticity Security policies bring another dimension of flexibility as they can define which factor or factors are required and under what circumstances (e.g., access to sensitive applications or a low behavioral assessment score triggers a request for another factor, for example, answer one or more challenge questions or enter an authorization code sent to the user's pre-registered cell number).
Cost	By supporting multiple authentication factors, all of which are not hardware-dependent at the user end, RSA Authentication Manager Express makes strong authentication a lower cost proposition, versus hardware-dependent factors, and highly scalable without requiring additional investments. Each RSA Authentication Manager Express platform can support up to 2,500 users.
User Convenience	There are several attributes of RSA Authentication Manager Express that support user convenience. Here are two: ▪ ***Risk-based authentication*** – With risk-based authentication, user authentication routines do not change unless the authentication attempt is determined to be high risk, at which point additional authentication factors are requested. Otherwise, the user's password and personal computer ID (transparently collected) are sufficient. The RSA Risk Engine, an embedded component of RSA Authentication Manager Express, creates a personalized behavior profile for each user to assess authentication risk. Being personalized, the user will be requested to present an additional factor only when there is a profile deviation. Furthermore, the user's profile is continuously updated based on his/her access and authentication activity and the activity of the user's group (e.g., members of the same department). This too limits the occasions a user is required to present additional authentication factors. ▪ ***Tokenless Authentication Factors*** – There is no need for the user to tote single-purpose authentication devices (e.g., a USB token or OTP key fob). Two devices the user already carries—personal computer for its device ID and cell phone to receive an authentication code—and the ability to answer challenge questions each represent an additional factor in a multi-factor authentication process.
Administrative Ease	Several elements of the RSA Authentication Manager Express platform ease administrative effort without depreciating its risk management capacities. ▪ An intuitive administrative portal contributes to a rapid "plug it in and go" experience for administrators. ▪ There is no software to install or hardware to configure on users' devices. ▪ Transparent profile creation and dynamic profile updates limit administrative interaction with regard to user provisioning and on-going management. ▪ The lengthy tenure and broad adoption of RSA Risk Engine serves to eliminate administrators' trial and error effort in establishing appropriate security policies based on behavioral analysis. ▪ The RSA Authentication Manager Express platform is currently out-of-the-box integratable with leading SSL VPN gateways (Juniper, Citrix, Cisco, and Check Point) and web applications (SharePoint, Outlook Web Access, etc.).

Stratecast

The Last Word

We live in a connected world. But it's also a disconnected world—disconnected in the sense that knowing who is on the other end is fraught with uncertainty. Resolving this dilemma is the role of strong authentication, specifically multi-factor authentication.

Historically, multi-factor authentication has carried with it baggage—user inconvenience, administrative headaches, and burdensome costs. For these reasons, many small and mid-sized businesses have taken on untold amounts of risk by relying solely on passwords to authenticate their system-accessing users. But this risk is no longer tolerable; a transition to multi-factor authentication is long overdue.

RSA Authentication Manager Express breaks through the barriers that have stopped businesses from augmenting password-based authentication with multi-factor authentication. RSA accomplishes this through a combination of tokenless authentication factors, behavioral analysis, risk-based authentication, and plug-and-play implementation and administration.

For small and mid-sized businesses, now is the time to take a fresh look at multi-factor authentication. Don't wait for an incident to occur.

RSA Authentication Manager Express breaks through the barriers that have stopped businesses from augmenting password-based authentication with multi-factor authentication.

Michael Suby

VP of Research
Stratecast (a Division of Frost & Sullivan)
msuby@stratecast.com

CONTACT US

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Beijing

Bengaluru

Bogotá

Buenos Aires

Cape Town

Chennai

Delhi

Dubai

Frankfurt

Kolkata

Kuala Lumpur

London

Manhattan

Melbourne

Mexico City

Milan

Mumbai

Oxford

Palo Alto

Paris

Rockville Centre

San Antonio

São Paulo

Seoul

Shanghai

Singapore

Sydney

Tel Aviv

Tokyo

Toronto

Warsaw

ABOUT STRATECAST

Stratecast assists clients in achieving their strategic and growth objectives by providing critical, objective and accurate strategic insight on the global communications industry. As a division of Frost & Sullivan, Stratecast’s strategic consulting and analysis services complement Frost & Sullivan's Market Engineering and Growth Partnership services. Stratecast's product line includes subscription-based recurring analysis programs focused on Business Communication Services (BCS), Consumer Communication Services (CCS), Communications Infrastructure and Convergence (CIC), OSS and BSS Global Competitive Strategies (OSSCS), and our weekly opinion editorial, Stratecast Perspectives and Insight for Executives (SPIE). Stratecast also produces research modules focused on a single research theme or technology area such as Connected Home (CH), MS and Service Delivery Platforms (IMS&SDP), Managed and Professional Services (M&PS), Mobility and Wireless (M&W), and Secure Networking (SN). Custom consulting engagements are available. Contact your Stratecast Account Executive for advice on the best collection of services for your growth needs.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best-practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 40 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.