TAKING CONTROL OF THE DIGITAL AND MOBILE USER AUTHENTICATION CHALLENGE

More websites, more mobile devices, more user accounts. It all adds up to more passwords and more access pathways. Traditional password strategies just aren’t keeping pace with the evolving landscape, where identity is increasingly a critical threat vector. The challenge is complex, complicated not just by rapidly changing user needs, but also by the information they need to access and the devices they use. This Technology Dossier examines the growing demands on authentication systems and the issues IT is struggling with to protect digital assets and retain control, while achieving the desired user experience.
Taming the Password Jumble

ENTERPRISES MUST STEP UP THEIR AUTHENTICATION STRATEGIES TO KEEP PACE WITH MARKET DEMANDS AND BETTER MANAGE RISKS.

Businesses are increasingly creating new services to grow revenue, drive productivity and innovation, and boost satisfaction. The confluence of mobile, social, cloud and big data technologies is creating new opportunities and channels to conduct business and engage with customers.

In response, enterprises have been particularly quick to provide mobile device access to online resources, either in the form of native mobile applications or Web-based access that adapts to different device formats. From email to human resources management systems, ERP to consumer checking accounts, businesses are embracing the flexibility of mobility by utilizing software applications hosted in the cloud, providing Web-based portals for employees and self-service portals for customers.

Meanwhile, a new mobile-ready enterprise has emerged. Traditional boundaries have dissolved under an onslaught of IT outsourcing, cloud services, workforce mobility initiatives, bring-your-own-device (BYOD) policies and the availability of corporate applications and data to remote workers and partners.

And these enterprises are reaping the rewards of mobility. According to the IDG Enterprise survey "Consumerization of IT in the Enterprise (CITE),” 70 percent of the more than 1,100 participants report that they have seen ROI from using consumer devices in the workplace, and more than half say external customer satisfaction was positively impacted. But mobility comes with a dark side—one out of four fraud transactions originate in the mobile channel.¹

Cybercriminals can be creative when it comes to uncovering those passwords, even the strong ones. They may be able to gain unauthorized access to corporate systems by installing malware on a mobile device, guessing a relatively simple password or gaining access to a user’s login credentials that are used on multiple systems.

Sometimes cybercriminals fool users into giving up credentials by using “phishing” emails that, when activated, either infect the user system with malware or lure the user to a bogus website, such as a fake bank portal, and then ask for a username and password. It’s been estimated that more than 37 million Internet users faced phishing attacks between early 2012 and early 2013, up from just less than 20 million a year earlier.³

Many users make it easy for the crooks, often choosing simple, commonly applied passwords, to bridge the gap. Although "password" is no longer the most used password on the Internet, it has been surpassed by an equally "hackable" string of characters: “123456.”⁴

Password management also makes for risky behavior. Whether it’s writing the username and/or password combination on the proverbial sticky note,⁵ or in an electronic address book,⁶
convenience often wins out over secure practices. That may seem unsophisticated, or even quaint. But in the era of BYOD, when employees regularly use personally owned devices to check, download, upload and share important content on corporate systems, the risk is real and severe.

Worse, they may be using the same username and password across multiple Web servers, a risk highlighted by the Heartbleed scare of early 2014 that resulted in vulnerability of encrypted credentials. According to Forrester Research, four out of five organizations still rely on username and password to secure access to consumer-facing portals. Administrators sometimes are just as culpable. Some reuse the same passwords and share them with other administrators, or neglect to change factory default—or publicly known—passwords for various equipment such as routers and POS devices. Amazingly, for about two decades during the height of the Cold War, the secret unlock code, or passive action link, to activate U.S. nuclear missile launches was “00000000.”

What’s more, the global consulting firm KPMG found that major organizations fail to check and remove metadata for the Web pages and documents that they publish online, providing information that researchers used to expose an average of 41 internal usernames and 44 email addresses per company.

In the end, poor management of credentials puts a strain on already burdened IT resources. Gartner analysts, for example, estimate that password issues account for 20 percent to 30 percent of all IT service desk volume.

### ASSURED AUTHENTICATION

Authentication management is another issue. As enterprises go mobile and make more online resources available to internal users, partners, vendors and customers, increasing demands for ready access creates a conflict with IT’s need to control who can access what information from which device in what locations. The ability to ensure proper authentication is getting more and more complex.

With users accustomed to switching between multiple devices—smartphones, laptops, tablets—the growing popularity and demand for mobile access exacerbates what was already a problem of ensuring proper use of password security. Standardized access restricted to a few select models of PCs and laptops is, for most, just a distant memory.

“Organizations have now pushed so much critical information out to the Internet that they now have this collision course of passwords as they are traditionally used,” says Jeffrey Carpenter, manager of product marketing for authentication with RSA, The Security Division of EMC. “Anybody can hit a Web page to log on to any company’s VPN or portal if they have the password.”

### AUTHENTICATION SPANNING ENVIRONMENTS

RSA has developed a suite of solutions to help resolve complex identity and access management challenges in this era of mobile, social, cloud and big data:

- **RSA SecurID**—multifactor, one-time password authentication technology for secure access to virtual private networks, wireless access points, remote access firewalls, Web applications and network operating systems.

- **RSA Adaptive Authentication**—exploring risk-based approach to multifactor authentication using device forensics, behavioral analysis and RSA eFraudNetwork.

- **RSA Identity Manager and Governance (IMG)**—enterprise-wide visibility into user access privileges, with automated reporting, monitoring and auditable compliance evidence.

- **RSA Access Manager**—secure access to Web applications with consolidated access controls for enhanced security, accelerated application deployment and improved user experience.
That puts identities at risk. In fact, according to Verizon’s annual report on data breach investigations, the use of stolen credentials topped the list of threat actions in 2013 for the first time in the five years of reporting.

There are also opposing mandates to ensure ease of use while at the same time managing risk in a secure and cost-effective manner. For example, mobile devices and BYOD was identified as the top security challenge by leading security decision makers who participated in CSO’s annual “State of the CSO” survey. That concern even surpassed cyberthreats from outside the organization.

In the past, such concerns might spur efforts to ratchet up access controls, but enterprises are just as concerned about making it easy for workers to conduct their business and for customers to access resources. With new technologies emerging first in the consumer market and then spreading to business organizations, employees expect—perhaps demand—the ease of use they are accustomed to in their private lives to spill over into their work environments.

In fact, EMC conducted a global survey of more than 15,000 participants that assessed consumers’ willingness to trade some privacy for more benefits or conveniences associated with digital technology. The study revealed that while more than half have experienced potentially compromised privacy due to a data breach, they are not taking basic measures to protect their information, such as regularly changing passwords or using password protection on mobile devices.

What’s more, EMC found that viewpoints on privacy varied wildly based on which of their online personas were affected—for example, Social Me for interaction with social media and email is least willing to trade privacy for convenience; while Consumer Me, interacting with online stores, is somewhat more tolerant; and Employee Me is just a little more tolerant interacting with employment-related systems and websites.

**OVERWHELMED**

The need to deal with multiple digital identities and the interconnection of resources inside and outside of the organization is overwhelming traditional access and authentication management practices. The result: increased complexity and new risks to manage on a number of fronts.

For starters, “The universe of what an organization consider ‘users’ has grown exponentially,” says Carpenter. “It includes auditors, vendors, suppliers—literally the world. Most organizations are struggling with trying to match the right authentication method to the right use.”

The proliferation of access pathways often results in disparate policies that increase the risk; for example, many organizations require two-factor authentication for VPN access, but users may be able to access the same resources from their mobile devices simply by entering a four-digit PIN. Organizations are seeking to regain control over such inconsistencies.

Further complicating security management is the threat of Shadow IT—the ability of users or individual departments to self-provision cloud services, such as file sharing or specific business services, with or without IT’s knowledge or approval. Not only are these services accessed without any approved authentication requirements, but users may reuse internal passwords on external cloud services, increasing the potential for passwords and usernames stolen from an external service being used to breach corporate assets within the firewall or on hosted enterprise services.

One-size-fits-all access and authorization management solutions no longer hold up when users and customers have so many options. “It’s an issue of being able to fit the right authentication method to the right user, to the right device, to the right information they are trying to access,” says Amy Blackshaw, manager of product marketing for fraud and risk intelligence with RSA. “It’s all about choices.”

CIOs and CFOs are faced with managing a spectrum of risk, based on who, how and from where access is being requested. More stringent security may apply to those who are coming in on the corporate network to access proprietary information, compared to more transparent security for those accessing a company’s social media.

Blackshaw notes that while an enterprise may be
able to exert more stringent controls over workers, it may not have much influence with consumers who resist added friction in their online activities. “Unlike employees, consumers can vote with their feet and seek out other service providers [that] they view as easier to deal with,” she says. Banks, for example, are struggling with the issue of how to provide consumer ease of access while ensuring security and confidentiality of their accounts. Similarly, healthcare organizations are rapidly rolling out patient portals while attempting to make authentication seamless and transparent.

**FORWARD PROGRESS**

KAYVAN ALIKHANI
Senior Director of Technology at RSA focusing on mobility

**Q.** It seems that virtually everybody is unhappy with today’s password-dependent authentication schemes, so what is RSA’s forward-looking, next-generation vision for resolving this?

**A.** The future is truly about choice and providing secure authentication that makes it easy for users to comply with security policies. In the past, biometrics wasn’t very convenient, and proved very expensive. Now cost-effective technologies built into mobile devices, such as the camera, speaker, accelerometer, fingerprint sensor and geolocation, can enhance authentication with behavior metrics based on the activities of the user, enabling a more convenient experience. Potential user authentication technologies include fingerprint, face or voice print, iris structures, ear shape, heartbeat analysis as well as activities such as keystroke analysis and handwriting.

**Q. How does behavior metrics differ from biometrics?**

**A.** It’s all about utilizing what a person is doing—tied with their mobile device—to better prove that they are who they say they are. With behavior metrics, you can look at who your users are, what they are trying to access, and where they are trying to access it. You need to have an ecosystem to deliver different controls based on those three groups, and flexibility for users. For example, in a dark room the smartphone camera is not going to “pick up” the face; in a loud subway, voice recognition probably won’t work; in police, fire and health vehicles where gloves are often worn, fingerprint sensor is not optimal. So you need options, almost like a menu, to give users choices. Even when people type onto their device or laptop keyboard, they have a specific signature based on velocities, rhythms and pressure. If you identify these factors passively, you get very rich indicators that enable frictionless authentication.

**Q. So how do we get from here to there, and what is it going to cost?**

**A.** Whether we realize it or not, what we’re going through here is the death of passwords. RSA’s vision is to evolve technology to meet the changing needs of organizations and protect them as they move into the realms of cloud, mobile, social and big data. It requires an organization with the ongoing vision and an ecosystem of partnerships that implies protocols and standards, not another point solution vendor that can provide the cheapest option. With cloud, for example, all of these organizations are going to be communicating, authenticating and cross authenticating, so you have to have protocols and standards to make that happen.

Organizations want something that is cheap to deploy, that is convenient to users and will protect all their information. Of course, that doesn’t exist. You have information and you don’t want that circulating freely on the Internet, so there is a value to protecting that information.

**Evolving Strategies in the Real World**

IT must develop authentication strategies that evolve with market changes. “If an employee at work can’t share photos or documents with acquaintances, they will find a way to send them through consumer-grade software that they like and are used to,” says Mushegh Hakhinian, lead security architect at Intralinks.

Intralinks provides strategic collaboration solutions on which more than $23 trillion in transactions
have been conducted and which incorporate RSA’s Adaptive Authentication Risk-Based Authentication Platform. Serving a wide range of industries, including financial services, life sciences, technology and manufacturing, Intralinks is able to provide multifactor authentication, without requiring users to manage individual tokens.

“The second identification factor is not something the user holds in hand; it is the device they originate a transaction from,” says Hakhinian. The authentication process can determine key behavioral aspects such as the network being used, a geolocation signal, or history of previous activity to determine likely fraudulent access attempts.

Analyst Jack Gold of J. Gold Associates, writing in a recent report on an identity-driven approach to mobile security, states, “A balanced approach between what users value highly and what IT requires to maintain security is an ongoing challenge that can best be addressed through a set of realistic and consistent policies, and security solutions that work in conjunction with these policies.” By establishing a unique user’s identity and current conditions, he adds, security can be tailored to the situation.

Finding that balance is an imperative for today’s enterprise. The vast majority of enterprises, particularly those that are consumer focused, still rely on simple username and password combinations, Blackshaw says. Many are familiar with RSA’s SecurID hardware-based authenticators that provide an easy-to-use, convenient, self-contained method for effective user identification. When users attempt to log in, they are required to provide something they know—a PIN—and something they have—a unique one-time password (OTP) from their SecurID token that changes every 60 seconds—before they are granted access to the secured application.

The time-based algorithm found in RSA hardware authenticators can also be utilized as software-based tokens that are bound to users’ mobile devices. The user experience is similar, although with the software tokens, once the PIN is entered, the one-time password appears on the device screen, to be copied into the particular access interface that is being used.

Companies like Intralinks that utilize tokens are now able to enhance security by utilizing RSA’s Risk Engine, which examines a variety of indicators to determine a user’s level of risk. Indicators could be something like an access request from a foreign location that a user is not likely to be in, or too-frequent requests from a single user coming from multiple time zones.

**BOTTOM LINE**

Passwords have been a mainstay—and a prime risk factor—since the era of the mainframe. Keeping pace with the latest cyberthreats, technology trends and business requirements calls for a change in traditional information security processes. Managing security and access management across increasingly diverse physical, virtual and cloud-based environments broadens the risk environment and creates new challenges.

Migrating to a risk-based authentication system increases security transparently by delivering multifactor authentication in a user-friendly fashion that improves the experience while ensuring that the right person gains access to the right information from an appropriate location and device. In order to achieve the desired balance between security and a positive user experience, organizations need an adaptive approach to identity and authentication that can adjust to changing needs and changing user behaviors. Only then can they securely embrace the mobile revolution without immobilizing the user.
Case Studies

ADP

ADP enables secure home working with RSA® Authentication Manager 8.0

As one of the world’s largest providers of business outsourcing and human capital management solutions, ADP offers human resource, payroll, talent management, tax and benefits administration solutions from a single source. It has more than $10 billion in revenues.

KEY REQUIREMENTS

Among the most sensitive data is that relating to employees. Employers typically hold information on their people that spans money, health, where they live, their banking and tax details, and their progress at work. ADP provides human capital management solutions to companies in more than 125 countries. “Security is essential to our business proposition,” said Rodrigue Klock, IT Security Engineer at ADP. “We have to prove to our customers that we are secure, so that they can have confidence they can work with us. We trust RSA SecurID to ensure our systems can only be accessed by authorized users.”

ADP has been using RSA SecurID for more than eight years in Europe, and for 15 years in the U.S. SecurID is the market-leading one-time password technology, interoperable with over 350 third-party applications. ADP uses hardware tokens to provide secured access for 400 customers to its computer systems.

Software tokens were distributed through RSA Authentication Manager using the Cryptographic Token Key Initialization Protocol (CT-KIP), but this required employees to connect to the local area network (LAN) to receive a token, so it could only be used when on site at an ADP office. Users at home would have to be manually emailed a software token or use a fixed passcode, which is less secure than a one-time password.

ADP needed a way to provide secure access to its systems for employees working from home or client sites, and connecting to the computer systems using VPN.

SOLUTION

ADP tested RSA Authentication Manager 8.0, the latest version of the software used to manage its secure network access. “RSA Authentication Manager 8.0 provides a better experience for our users because they don’t have to be in the office to receive a software token anymore,” said Klock. “They can download it directly over the Internet when connected to the VPN or using VPN-SSL, without compromising on security. Users enter their personal identification number (PIN) into the software on their computer, and this creates the passcode that is used to connect. As a result, they can work securely anywhere they can get online.”

He adds: “The design of RSA Authentication Manager 8.0 is much simpler for administrators to use than the previous version. The new interface brings a lot of information together in one place. Previously, you would have to click several times to see a user profile, token details, and date of connection, but now all that information can be found on a single screen that brings together the global information on users.”
BRE LEASING

BRE Leasing achieves secure mobility with RSA Authentication Manager 8.0

Leasing is a process by which a firm can obtain the use of a certain fixed asset for which it must pay a series of contractual, periodic, tax-deductible payments. Confirmed by the Polish Leasing Association as one of Poland’s leading companies in the leasing sector, BRE Leasing provides its clients with lease solutions that help to optimize and develop their businesses. It offers a wide range of comprehensive, standardized services for SMEs and larger companies alike. www.bre-leasing.pl

KEY REQUIREMENTS

We are all functioning in an increasingly mobile environment. The growth of mobility brings with it the opportunity for employees to use their devices on-the-go to boost efficiency and flexibility, while also opening new doors for sales, business development, and customer relations. In order to embrace these opportunities, employees need to be able to access all of their usual applications and servers through their mobile devices.

The management team at BRE Leasing wanted to capitalize on these opportunities. In fact, not doing so could be costly for the business, as explained by Eligiusz Łasica, Specialist of IT Infrastructure, BRE Leasing. “The idea of losing potential customers as a result of reduced mobility is not an impossibility. With the sales process, it is important to strike while the iron is hot — and that iron can cool if you need to travel all the way back to a specific office to complete a deal.” Without providing a remote-access portal, BRE Leasing was worried that a lack of mobility and flexibility would have a negative effect on the sales team and thus the business as a whole.

However, the company was concerned about the security issues that come with Bring Your Own Device (BYOD) initiatives. It decided that it needed an authentication system that was strong, yet flexible, and would allow staff to gain secure, remote access to business information 24 hours a day, seven days a week. The efficiency of a potential authentication system needed to be factored in for the sake of the IT department. Sławomir Ostrowski, Deputy Director for Exploitation and IT Systems Security, BRE Leasing, explains: “Today’s business functions on mobile platforms, and companies need to adapt accordingly. This would be a simple strategy if security wasn’t an issue, but it is. We were looking for something that would allow our staff to access our business information from anywhere, at anytime — but securely and without placing too much of a burden on our IT support team.”

SOLUTION

BRE Leasing made the decision to facilitate its new mobile working set up with RSA Authentication Manager 8.0. The team was particularly attracted to the flexibility it offers, including more authentication choices for end users, as well as the simplicity of managing the virtual platform. “We have been with RSA since around 2006. We have always been impressed with the RSA team and technologies over our long working relationship,” says Ostrowski. “The decision to migrate to the latest version of RSA Authentication Manager was automatic. It was not a question of ‘if’, but ‘when’ we were going to upgrade.”
GEISINGER HEALTH SYSTEM

Transforming patient care in the Emergency Department

Founded in 1915, Geisinger Health System is a physician-led healthcare system, dedicated to healthcare, education, research, and service, spanning 41 counties in Pennsylvania and serving 2.6 million people. It has received national recognition as a model for best-practice health services delivery and its physicians have been listed in The Best Doctors in America. To learn more, please visit: www.geisinger.org.

KEY REQUIREMENTS

Geisinger Health System is a nationally recognized leader in healthcare IT, specifically the adoption of electronic patient records to improve patient care. It has an extensive network of departmental applications and web portals serving staff, affiliated physicians, patients, and health-plan members.

Geisinger has long used access management software to provide physicians and patients with single sign-on access to clinical applications as well as authentication tokens to provide additional secure access for employees and vendor partners.

To further improve the quality and safety of patient care, Geisinger put in place a program to integrate and extend access to its network of healthcare IT systems. It recently created a Regional Health Integrated Organization (RHIO) connected via The Keystone Health Information Exchange (KeyHIE™).

The aim of KeyHIE is to allow clinicians at some 53 rural Pennsylvania hospitals to easily share patient data. The first phase of this project is a pilot implementation involving the Emergency Departments (ED) at Geisinger Medical Center, Shamokin Hospital, and Bloomsburg Hospital, all located in north central Pennsylvania.

SOLUTION

Geisinger selected RSA Access Manager and RSA Federated Identity Manager to manage user access across the three hospitals. This enterprise-ready solution enables organizations to securely exchange identities across network domains, providing end users with secure access to multiple external applications with a single identity and log on.

The system allows doctors and nurses in the Geisinger, Shamokin, and Bloomsburg emergency departments to access critical health data of each other’s patients in real time. Using RSA technology, Geisinger has been able to mitigate the risk of internal security breaches through centralized management and control of user authentication and authorization privileges.

Geisinger has also rolled out RSA Adaptive Authentication to provide affiliated and referring physicians with secure access to patients’ electronic medical records. The solution’s risk-based authentication technology conducts a risk assessment behind the scenes, ensuring minimal inconvenience to the user.

A unique risk score is assigned to each activity, and users are only challenged when an activity is identified as moderate or high risk and/or an organizational policy is violated.

David Young, IT Director at Geisinger Health System, says: “We were particularly attracted by the way RSA Adaptive Authentication offers layers of security in addition to the standard user name and password, but without inconveniencing the user. It is ideal for clinicians working in a busy and often pressured hospital and clinic environment.”
RAPATTONI

Rapattoni builds business by protecting customer interests

Rapattoni is one of the leading software providers for the U.S. real estate industry. Established in 1970, the company provides the technology to power more than 100 Multiple Listing Services (MLS) which are in turn used by more than 250,000 real estate professionals to share information about properties for sale.

KEY REQUIREMENTS
An MLS, which consists of hundreds of data fields that provide real estate agents with information relating to listed properties, is an indispensable tool for U.S. real estate agents.

Rapattoni provides its MLS service via a Software-as-a-Service (SaaS) model, ensuring MLSs receive frequent software updates. Several years ago, Rapattoni implemented a market-leading strong authentication system based on software and hardware tokens to allow MLSs to protect their systems from unauthorized use. The implementation was a great success, with a large number of real estate professionals using tokens for secure website access to safeguard clients’ personal information.

Rapattoni was particularly interested when its trusted vendor launched a new adaptive authentication solution. This is a comprehensive authentication and fraud-detection platform that monitors and authenticates customer activity based on risk levels, institutional policies, and customer segmentation. As a result, Rapattoni was keen to incorporate the technology into its MLS offerings.

It believed the solution could galvanize existing security protection and equally importantly, in a small but intensely competitive market undergoing economic turmoil, Rapattoni understood that the solution could also be used as a market-winning business differentiator.

SOLUTION
Tim P. Johnson, Chief Financial Officer and VP of Business Development, Rapattoni, said: “The RSA SecurID® system is a great advantage for our MLS customers. In line with our philosophy of introducing innovative technologies, we also decided to offer our customers RSA Adaptive Authentication.”

RSA Adaptive Authentication establishes the identity of users by measuring a series of risk indicators such as device identification, geographical location, and behavioral profiling. By deploying the technology, Rapattoni’s customers ensured legitimate users can securely access the MLS from an office PC, notebook, or remote PC at a client site, regardless of location.

It works by collating fraud indicators with user profiling and transactional behavioral patterns and identifies behavior and activity patterns that do not conform to historical patterns and known activities. If the RSA Adaptive Authentication system does not recognize the IP address range, the user will need to answer a series of ‘challenge questions’ in order to be authenticated.

If the IP address range does not reflect common usage patterns, a series of further flags will also be raised, requiring more responses from the user before access is permitted. All incoming logon attempts are vetted against RSA’s eFraudNetwork™, the industry’s first and largest cross-institution, cross-industry, and cross-platform online fraud network dedicated to sharing and disseminating information on fraudulent activity.