Adventures and Ethics in MF Authentication

Thamraj Ghorsad*

raj.ghorsad@gmail.com

*M.Tech, Department of Computer Science & Engg.,

RGPV University, Bhopal, India

Abstract-

We are Seeing Adventures in MF Authentication that means Multi-factor authentication, It ensures that a user is who they claim to be. The more factors used to determine a persons identity, the greater the trust of authenticity. It serves a vital function within any organization - securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be. Â Evolving business needs around cloud applications and mobile devices, combined with rising threats, and the need to reduce costs, require entirely new considerations for access control. A ***strong authentication solution*** *that validates the identities of users and computing devices that access the non-public areas of an organization's network is the first step in building a secure and robust information protection system.*

Keywords—

MFA, Strengthen, Strong, threats, skydiving, mountain climbing, river rafting

INTRODUCTION

As the name starts with an Adventure An **adventure** is an exciting or unusual experience. It may also be a bold, usually risky undertaking, with an uncertain outcome. Adventures may be activities with some potential for physical danger such as skydiving, mountain climbing, river rafting or participating in extreme sports. The term also broadly refers to any enterprise that is potentially fraught with physical, financial or psychological risk, such as a business venture, a love affair, or other major life undertakings. **Multi-factor authentication** serves a vital function within any organization -securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be. Â Evolving business needs around cloud applications and mobile devices, combined with rising threats, and the need to reduce costs, require entirely new considerations for access control.

WHAT IS MULTI-FACTOR AUTHENTICATION (MFA)?

Multi-factor authentication ensures that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity.

Multi-factor authentication can be achieved using a combination of the following factors:

- *Something You Know – password or PIN*
- *Something You Have – token or smart card (two-factor authentication)*
- *Something You Are – biometrics, such as a fingerprint (three-factor authentication)*

Because multi-factor authentication security requires multiple means of identification at login, it is widely recognized as the most secure software authentication method for authenticating access to data and applications.

THE NEED FOR MULTI-FACTOR AUTHENTICATION

New threats, risks, and vulnerabilities as well as evolving business requirements underscore to the need for a strong authentication approach based on simple service delivery, choice, and future-forward scalability.

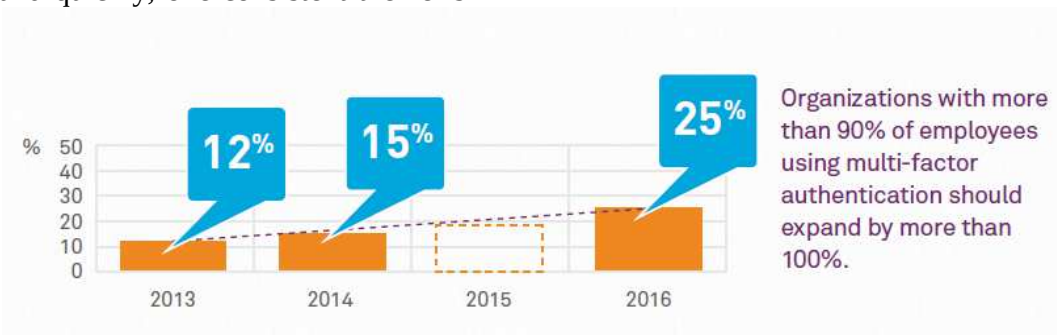
Now a days, organizations are asking:

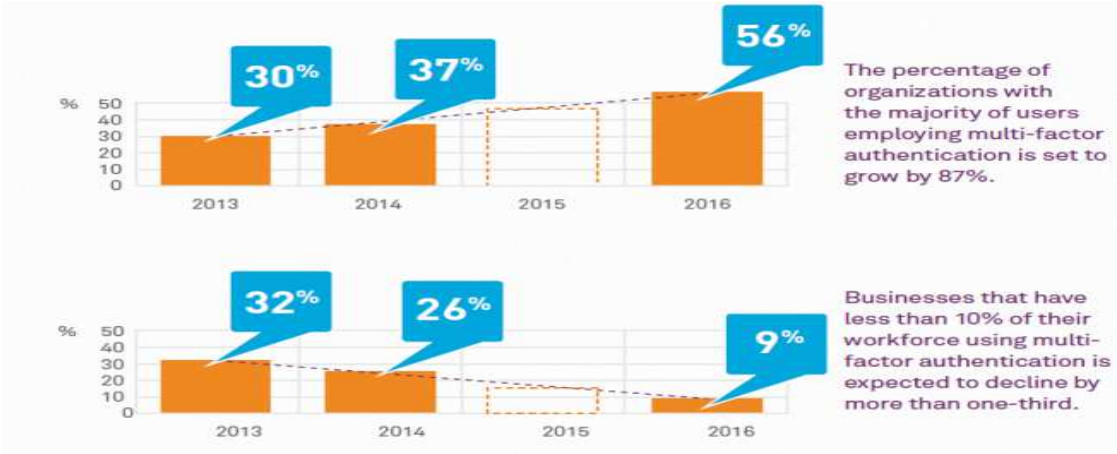
- Can I address new demands of my business â€" like cloud and mobile devices?
- How do I map authentication methods to business risk and the needs of my users?
- Can I centrally manage, control and administer all my users and endpoints?
- Who controls my authentication data?

- How can I incorporate additional security layers to help me further fortify against threats?
- And how do I keep it all practical and cost-effective?

EXPANDING USAGE OF MULTI-FACTOR AUTHENTICATION

While the technical and security landscape is shifting fundamentally and quickly, one consistent theme is emerging: Multi factor authentication will play an increasingly central role in an organization's security defenses. In this year's survey, respondents were asked about current multi-factor authentication adoption and anticipated usage in two years. Combined with our 2013 survey, we have three data points to track adoption rates, and across the board, usage is rising.





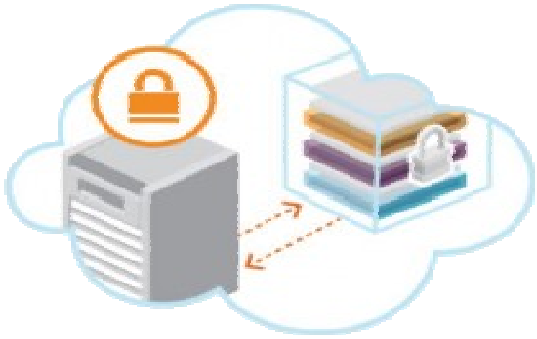
THE NEED FOR STRONG AUTHENTICATION

A **strong authentication solution** that validates the identities of users and computing devices that access the non-public areas of an organization's network is the first step in building a secure and robust information protection system. Strong authentication — also known as *two-factor authentication* — refers to systems that require multiple factors for authentication and use advanced technology, such as secret keys and encryption, to verify a user's identity. The simplest example of strong authentication is a consumer's ATM card. This requires something the user has (their card), and something they know (their PIN). Most people wouldn't want their bank to allow access to their checking account with just one factor.

Yet many organizations allow entrance to their valuable VPN, Citrix, and Outlook Web Access resources (often much more valuable than a single personal checking account) with only one factor—often a weak password. Strong authentication enables organizations to strengthen the protection of these vital resources.

While the decision to use strong authentication is clear cut, deciding on an approach is anything but. Today, there are hundreds of options, with each presenting its own specific advantages and tradeoffs.

HOW TO STRENGTHEN YOUR AUTHENTICATION?



SafeNet's multi-factor authentication software delivers the protection you expect, while enabling customers with broader choice, improved visibility, and the ability to expand into the future. We do this through our Fully Trusted Authentication Environment, which means that you have:

- **Better self-control of your data** - SafeNet enables customers with the option to create and control their own token data, so there is no reliance on a third-party vendor
- **Improved management and visibility** – SafeNet's solutions deliver single-server management, providing full control, simple administration, and reduced cost and staff burden
- **Expanded options** – SafeNet delivers the broadest choice when it comes to authentication methods – so you can meet the needs of any user and any risk level (hardware or software, certificate-based authentication or traditional one-time-password, on-premise, or into the cloud)
- **Future-ready** - SafeNet provides new solutions that deliver strong authentication and single sign-on (SSO) for cloud applications as well as credentialing for mobile device management

- **Painless migrations** - SafeNet offers seamless migration to cloud-based authentication, which maintain your existing investments and cause no disruption to end users

CONSIDERATIONS FOR SELECTING A MULTI-FACTOR AUTHENTICATION SOLUTION

With the plethora of strong and two-factor authentication offerings available today, it is important for organizations to carefully evaluate the available solutions before making a decision on which solution to implement. When choosing a strong authentication solution, organizations should take a number of factors into account. The following are some questions to consider:

- **Do I want to protect my internal network from unauthorized access?**

  If so, consider two factor authentication solutions that enable flexible and comprehensive secure network access, both in the office and remotely if needed.

- **Do my users need to connect from remote locations?**

  If so, consider portable solutions that enable secure VPN and web access for remote users, and that enable employees to secure their laptops and data while on the road.

- **Do my users need to access many password-protected applications?**

  If so, consider solutions that provide single sign-on functionality, either by storing user credentials on the token or by integrating with external single sign-on systems.

- **I want my users to digitally sign and encrypt sensitive data or transactions?**

  If so, consider smart card-based solutions that provide secure onboard PKI key generation and cryptographic operations, as well as mobility for users.

- **How sensitive is my business data?**

  The more sensitive the data, the higher the priority on the robustness and security of the solution.

- **Do I want to firmly protect data that sits on my users' PCs and laptops?**

  If so, consider token solutions that integrate with PC security products such as boot protection and disk encryption applications that require the use of a token to boot a computer or decrypt protected data.

- **Have I or do I want to implement a secure physical access solution?**

  If so, consider token solutions that enable integration with physical access systems.

SCOPE AND FOCUS

MF Authentication, or the act of proving that someone is who they claim to be, is a cornerstone of security. As more time is spent using computers, authentication is becoming both more common and increasingly important. Users must authenticate to prove their identity to maintain a continuous presence with a wide variety of computing services.

Our most common method of authentication continues to be based on the assumption of a person using a desktop computer and keyboard, or a person authenticating to their mobile phone -- what Bill Buxton has referred to as the "missionary position": one user and one computer face-to-face - no other position allowed. There has been an implicit assumption that the effort of authenticating, both in terms of elapsed time, user actions, cognitive load and impact on a user's primary task, will be amortized over a relatively long lifetime of the authenticated session with the system, application or service. As computing moves into new environments, including mobile and embedded systems, these assumptions may no longer be valid.

In the era of mobile, embedded and ubiquitous computing, the time for each interaction with a device, application or service is becoming much briefer. The user's primary task may be tending to a patient, driving a car, operating heavy machinery, or interacting with friends and colleagues via mobile apps. Due to the nature of user interaction in these new computing environments, and new threat models, methods of authenticating are needed that are both robust, easy to use, and minimize impact on the user's primary task. The time / cost of authentication needs to be commensurate with the level of engagement with these kinds of systems and applications.

The purpose of this workshop is to bring together researchers and practitioners to share experiences, concerns, and ideas about known and new authentication techniques. We are interested in discussing methods of evaluating the impact and usability of various authentication techniques, and ideas about novel authentication techniques that are secure, robust and usable.

The goal of this workshop is to explore these and related topics across the broad range of contexts, including enterprise systems, personal systems, and especially mobile and embedded systems (such as automotive and wearable systems). This workshop provides an informal and interdisciplinary setting at the intersection of security, psychological, and behavioral science. Panel discussions may be organized around topics of interest where the workshop participants will be given an opportunity to give presentations, which may include current or prior work in this area, as well as pose new challenges in authentication. Topics of interest include:

- Surveys and comparisons of known authentication techniques
- Novel metrics or comparisons of metrics for authentication strength
- Empirical evaluations of authentication techniques, including performance, accuracy, and the impact of authentication on a user's primary task
- New authentication techniques that target emerging computing environments such as mobile and embedded systems
- Approaches (including protocols) that enable weak authentication schemes to be more robust
- Existing authentication techniques applied in new environments or usage contexts
- Novel approaches to the design and evaluation of authentication systems

Researchers and practitioners interested in the topics outlined below. We expect that researchers from both industry and academia will find relevant material in the workshop.

KEY FINDINGS

Clear growth in multi-factor authentication (MFA) adoption:

- 37 percent of organizations now use MFA for a majority of employees – up from 30 percent last year
- By 2016, 56 percent of organizations expect the majority of users to rely on multi-factor authentication.

Cloud authentication gaining acceptance:

- 33 percent of organizations indicated they preferred cloud-based authentication, up from 21 percent last year – a 50 percent increase
- 33 percent is now open to the cloud for authentication implementations

MFA for mobile devices:

- More than 53 percent of respondents said users of mobile devices have restricted access to corporate resources.
- Those using MFA for mobile users, (22 percent currently) expect usage to grow to 33 percent by 2016 – an increase of 30 percent

"It's clear that some IT departments are struggling to keep up with the rapid pace of change caused by new technologies. The danger is that companies are unable to offer staff the full system access they require to perform their job because they don't have the secure authentication in place to allow access. Then there's the fact that almost every other week we hear about a new enterprise being hacked and data potentially leaked. So there is a perpetual battle to keep up with fast-paced advances in technology, and attempts to protect the company and curb security risks," stated Jason Hart, Vice President of Cloud Solutions at SafeNet.

Cost and Budget Priority

The 451 Research report revealed that authentication and identity access management are a top priority for security projects. Yet, interestingly, in the SafeNet Authentication Survey, almost 40 percent did not know how much their authentication solution costs per user per year, illustrating the lack of awareness over what is most cost-effective for the organization. The perception that, by not spending extra on multi-factor authentication, the organization is cost saving could be misleading to those in charge of IT budgeting. In fact, a multi-factor authentication solution aims to reduce authentication costs and improve ease of use.

Cloud vs. On-Premises-based Authentication

The growing demand from employees to connect to the corporate network with their own device has been met with a rise in cloud-based authentication from organizations. This year, 33 percent of companies indicated that they preferred cloud-based authentication, up from 20 percent last year.

"Ultimately, enterprises must accept that their staff will find ways to use mobile devices to access corporate data – with or without permission. Instead of preventing access, IT decision-makers need to deploy multi-factor authentication, which can offer the protection of corporate resources, while allowing staff access and maintaining productivity and performance," Hart added.

Authentication from Mobile Devices

When it comes to using strong authentication for mobile devices with access to corporate resources, the majority of responses were grouped at either end of the scale, showing polarized practices. Almost 40 percent said less than 10 percent of users are required to use strong authentication, while over 20 percent suggest that 90-100 percent of users currently require it. Interestingly, these figures are set to shift significantly, with 33 percent expecting that 90-100 percent of users will require strong authentication in the next two years, and only 15 percent suggest less than 10 percent, emphasizing the growing importance of mobile authentication.

The drive towards mobile authentication is also fuelling a move from hardware- to software-based authentication tokens. The survey revealed that the use of software-based authentication rose from 27 percent in 2013 to 40 percent in 2014, with the expectation that this will rise again to 50 percent in 2016. Conversely, the use of hardware-based authentication dropped from 60 percent in 2013 to 41 percent in 2014.

"IT companies are certainly responding to the rise in mobility with increased software-based authentication; however, there appears to be a 'disconnect' between the desire to embrace mobility, and the struggle to keep up with it and protect resources and data from external threats. Furthermore, as adoption of cloud computing grows, better security becomes crucial. Indeed, the cloud offers various benefits for authentication and applications, but without the security to support them, it only increases the threat." Hart concluded.

About the Survey

The research from SafeNet polled more than 350 senior IT decision-makers from around the world—about 29 percent from the Asia Pacific region; 42 percent from Europe, Middle East and Africa; and 29 percent from North America. The report compares data with a corresponding report from 2013. The full report can be found here: www.safenet-inc.com/resources/data-protection/2014-authentication-survey-executive-summary/

About SafeNet Data Protection Solutions

SafeNet data protection solutions provide multi-layer encryption with centralized key management and storage. SafeNet delivers the comprehensive encryption platforms that enable security professionals to safeguard sensitive data in data centers, virtualized data centers, and private and public clouds.

SafeNet enables customers to encrypt sensitive data at the storage, file, virtual instance, database, and application layer, while managing encryption security policies and encryption keys centrally. In addition, SafeNet supports format-preserving tokenization for a wide variety of data types. Through this multi-layer approach, SafeNet enables organizations to:
Separate administration of systems and applications from the data stored or processed within these infrastructure layers, ensuring privileged users can't see sensitive data.
Take advantage of lower cost operational models while consistently enforcing security policies.

- Centralize encryption management across physical, virtual, and public cloud environments, and efficiently deliver detailed logs and compliance reporting for internal and external auditors.
- Employ key vaulting and secure cryptographic resources, both in data center and multi-tenant environments, in order to retain full ownership and control of their encryption service.

With these capabilities, organizations can institute a defense-in-depth strategy that delivers high levels of security for sensitive data, regardless of where it resides—even if there has been a breach of other controls.

SafeNet Authentication Service

SafeNet Authentication Service is a cloud-based authentication solution that allows service providers and enterprises to rapidly introduce authentication-as-a-service to their customers. It also allows them to significantly reduce the cost and complexity associated with offering and implementing strong authentication, and to strengthen their security and compliance posture. This process is simplified through the flexibility and scalability of automated workflows, vendor-agnostic token integrations, and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless and enhanced user experience. With no infrastructure required, SafeNet Authentication Service enables a quick migration to a multi-tier and multi-tenant cloud environment, and protects everything from cloud-based and on-premises applications to networks, users, and devices.

CONCLUSION

In the authentication market, there's been plenty of change. In our survey, some clear patterns emerge. Most importantly, there will be more—more multi-factor authentication usage across the organization, and more usage from staff working on their mobile devices. These realities, coupled with the need to speed deployment and improve total cost of ownership, are clearly a big reason that cloud-based authentication, virtually an unknown a few years ago, is now the preference for more than 30% of respondents.

ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lectures who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

1. "Adventure". *dictionary.com*. Retrieved 2013-06-13.
2. Safenet (2014). Authentication Survey Executive Summary **How Organizations Are Responding to Mobile and Cloud Threats. Retrieved June 25, 2014** http://www.safenet-inc.com
3. D. Ilett (2005). US bank gives two-factor authentica-tion to millions of customers, Available at http://www.silicon.com/financialservices/0,3800010322,39153981,00.htm
4. D. de Borde (2008). Two-factor authentication,Siemens Enterprise Communications UK-Security Solutions, Available at http://www.insight.co.uk/files/whitepapers/Twofactor/authentication/ (White/paper).pdf
5. Korea Internet Security Agency (2010). Introduction of i-PIN (http://i-pin.kisa.or.kr),
6. Accredited Certificate: http://www.rootca.or.kr

7. Public Procurement Service: http://www.g2b.go.kr
8. Burr, W. E., Dodson, D. F., & Polk, W. T. (2004). *Electronic authentication guideline* (pp. 800-63). US Department of Commerce, Technology Administration, National Institute of Standards and Technology.
9. Internet X.509 Public Key Infrastructure Subject Identification Method (SIM), 2006.10.
10. OMB M-04-04, E-Authentication Guidance for Federal agencies , 2003, December, 16.