Multi-factor authentication

From Wikipedia, the free encyclopedia

Multi-factor authentication (**MFA**) is a method of computer access control which a user can pass by successfully presenting several separate authentication stages

Contents

Factors

Knowledge factors

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate, for example a password.

A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on password as one factor of authentication.[1]

A personal identification number (PIN) is a secret numeric password and is typically used in ATMs. Credit and ATM cards do not contain the PIN or CVV on the magnetic stripe.[2]

Secret questions such as "Where were you born?", are also a knowledge factor.

Possession factors

Possession factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems.

Several methods are used as possession factors:

Disconnected tokens

Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user.[3]

RSA SecurID token, an example of a disconnected token generator.

Connected tokens

Connected tokens are devices that are physically connected to the computer to be used, and transmit data automatically.[4] There are a number of different types, including card readers, wireless tags and USB tokens.[4]

Inherence factors

These are factors associated with the user, and are usually biometric methods, including fingerprint readers, retina scanners or voice recognition.[5]

Regulation

Details for authentication in the USA are defined with the Homeland Security Presidential Directive 12 (HSPD-12).[6]

Existing authentication methodologies involve the explained three types of basic "factors". Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods.[7]

IT regulatory standards for access to Federal Government systems require the use of multi-factor authentication to access sensitive IT resources, for example when logging on to network devices to perform administrative tasks[8] and when accessing any computer using a privileged login.[9]

Guidance

NIST Special Publication 800-63-2 discusses various forms of two-factor authentication and provides guidance on using them in business processes requiring different levels of assurance.[10]

In 2005, the United States' Federal Financial Institutions Examination Council issued guidance for financial institutions recommending financial institutions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing online financial services, officially recommending the use of authentication methods that depend on more than one factor (specifically, what a user knows, has, and is) to determine the user's identity.[7] In response to the publication, numerous authentication vendors began improperly promoting challenge-questions, secret images, and other knowledge-based methods as "multi-factor" authentication. Due to the resulting confusion and widespread adoption

of such methods, on August 15, 2006, the FFIEC published supplemental guidelines—which states that by definition, a "true" multi-factor authentication system must use distinct instances of the three factors of authentication it had defined, and not just use multiple instances of a single factor.[11]

Security

According to proponents, multi-factor authentication could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many multi-factor authentication approaches remain vulnerable to phishing,[12] man-in-the-browser, and man-in-the-middle attacks.[13]

Implementation considerations

Many multi-factor authentication products require users to deploy client software to make multi-factor authentication systems work. Some vendors have created separate installation packages for network login, Web access credentials and VPN connection credentials. For such products, there may be four or five different software packages to push down to the client PC in order to make use of the token or smart card. This translates to four or five packages on which version control has to be performed, and four or five packages to check for conflicts with business applications. If access can be operated using web pages, it is possible to limit the overheads outlined above to a single application. With other multi-factor authentication solutions, such as "virtual" tokens and some hardware token products, no software must be installed by end users.

Multi-factor authentication is not standardized. There are various implementations of it. Therefore, interoperability is an issue. There exist many processes and facets to consider in choosing, developing, testing, implementing and maintaining an end-to-end secure identity management system, inclusive of all relevant authentication mechanisms and their technologies: this context is considered the "Identity Lifecycle".[14]

There are drawbacks to multi-factor authentication that are keeping many approaches from becoming widespread. Some consumers have difficulty keeping track of a hardware token or USB plug. Many consumers do not have the technical skills needed to install a client-side software certificate by themselves. Generally, multi-factor solutions require additional investment for implementation and costs for maintenance. Most hardware token-based systems are proprietary and some vendors even charge an annual fee per user. Deployment of hardware tokens is logistically challenging. Hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed. In addition to deployment costs, multi-factor authentication often carries significant additional support costs. A 2008 survey (http://www.cujournal.com/issues/12_15/-100094-1.html) of over 120 U.S. credit unions by the *Credit Union Journal* reported on the support costs associated with two-factor authentication. In their report, software certificates and software toolbar approaches were reported to have the highest support costs.

Examples

Several popular web services employ multi-factor authentication, usually as an optional feature that is deactivated by default.[15]

See also

- Identity management
- Mutual authentication
- Reliance authentication
- Strong authentication

References

1. "Securenvoy - what is 2 factor authentication?" (https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm). Retrieved April 3, 2015.
2. "Information technology -- Identification cards -- Financial transaction cards" (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317). *ISO/IEC 7813:2006*.
3. de Borde, Duncan. "Two-factor authentication" (http://web.archive.org/web/20120112172841/http://www.insight.co.uk/files/whitepapers/Two-factor%20authentication%20(White%20paper).pdf) (PDF). Archived from the original (http://www.insight.co.uk/files/whitepapers/Two-factor%20authentication%20(White%20paper).pdf) (PDF) on January 12, 2012.
4. van Tilborg, Henk C.A.; Jajodia, Sushil, eds. (2011). *Encyclopedia of Cryptography and Security, Volume 1*. Springer Science & Business Media. p. 1305. ISBN 9781441959058.
5. Biometrics for Identification and Authentication - Advice on Product Selection (http://www.cesg.gov.uk/publications/Documents/biometricsadvice.pdf)
6. US Security Directive as issued on August 12, 2007 (http://hspd12.usda.gov/about.html)
7. "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment", August 15, 2006
8. "SANS Institute, Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches" (http://www.sans.org/critical-security-controls/control.php?id=10).
9. "SANS Institute, Critical Control 12: Controlled Use of Administrative Privileges" (https://www.sans.org/critical-security-controls/control.php?id=12).
10. "Electronic Authentication Guide" (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf) (PDF). *Special Publication 800-63-2*. NIST. 2013. Retrieved 2014-11-06.
11. FFIEC (2006-08-15). "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment" (http://www.ffiec.gov/pdf/authentication_faq.pdf) (PDF). Retrieved 2012-01-14.
12. Citibank Phish Spoofs 2-Factor Authentication (Brian Krebs, July 10, 2006) (http://voices.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html)
13. The Failure of Two-Factor Authentication (Bruce Schneier, March 2005) (http://www.schneier.com/blog/archives/2005/03/the_failure_of.html)
14. The Identity Lifecycle, Part 1 (Brent Williams, 2010) (http://www.anakam.com/News/Blog/Technical/15/Identity-Lifecycle-part-1/)
15. GORDON, WHITSON (3 September 2012). "Two-Factor Authentication: The Big List Of Everywhere You Should Enable It Right Now" (http://www.lifehacker.com.au/2012/09/two-factor-authentication-the-big-list-of-everywhere-you-should-enable-it-right-now/). *LifeHacker* (Australia). Retrieved 1 November 2012.

External links

- Attackers breached the servers of RSA and stole information that could be used to compromise the security of two-factor authentication tokens used by 40 million employees (register.com, 18 Mar 2011) (http://www.theregister.co.uk/2011/03/18/rsa_breach_leaks_securid_data/)
- Banks to Use Two-factor Authentication by End of 2006 (http://it.slashdot.org/article.pl?sid=05/10/19/2340245&tid=172&tid=95), (slashdot.org, 20 Oct 2005)
- List of commonly used websites and whether or not they support Two-Factor Authentication (http://twofactorauth.org/)

- Microsoft to abandon passwords (http://web.archive.org/web/20081011073929/http://www.vnunet.com/vnunet/news/2126966/microsoft-abandon-passwords), Microsoft preparing to dump passwords in favour of two-factor authentication in forthcoming versions of Windows (vnunet.com, 14 Mar 2005)
- Why is two factor authentication needed for your corporate assets (http://www.celestix.com/assets/documents/HOTPin/Whitepaper/Securing_Corporate_Assets_with_2FA.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Multi-factor_authentication&oldid=670527292"

Categories: Authentication methods | Computer access control
