FORTINET

Solution Brief

The Password as you Know it is Dead:

Welcome to the World of Two-Factor Authentication

In 2012, researchers at Fortinet's FortiGuard Labs published a report that predicted a marked increase in businesses migrating to two-factor authentication in 2013. Three months into the New Year, after a data breach forced the company to reset 50 million of its users' passwords, Evernote announced plans to adopt two-factor authentication as a better means of securing its users' data. Other companies that have also recently made that transition include Amazon, Apple, Dropbox, eBay, Facebook, Google and Microsoft.

According to TechNavio, the global two-factor authentication market is expected to grow 20.8% between 2011-2015 (1). According to Markets and Markets, the multi-factor authentication market will reach $5.45 billion by 2017(2). Finally, Fortinet's FortiAuthenticator platform, which complements the FortiToken range of two-factor authentication tokens for secure remote access, has recently seen triple digit growth.

Why Single Factor Authentication is Doomed

"In the early days of Internet authentication, plain text passwords were often sufficient, as the number of threat vectors were minimal and processing horsepower and password repositories weren't readily available to just anyone," said Richard Henderson, security strategist and threat researcher for Fortinet's FortiGuard Labs. "As newer password cracking tools, faster processors and always-on Internet connections arrived, plain text passwords started to come under fire. With the advent of cloud cracking services, such as Cloud Cracker, which leverages the power of distributed computing, 300 million password attempts can be made in as few as 20 minutes for around

Challenges

- With recent increases in processing power and the ability to outsource password cracking to the cloud, password-only based authentication is no longer sufficient to secure your critical data.
- There are currently four ways to manage passwords, none of which are completely infallible. This necessitates the need for businesses to investigate multiple factors of authentication.

Objectives

- Understand the multiple factors of authentication available today, the pros and cons of each and determine the best ones to choose for your environment and unique business requirements.

Implementing two-factor authentication lets you solve network authentication security problems affordably by adding a second factor for strong authentication. You cannot always trust your users with your network security. Relying solely on static passwords for remote access to your VPN and web sites provides only weak authentication, because your users' passwords are vulnerable to theft or guessing, as well as dictionary and brute-force attacks.

$17, meaning even a strong, encrypted password can be cracked with a little patience."

There are basically four ways to manage network passwords today and none of them are invulnerable on their own:

1. **Plain Text:** This is the weakest method of password management, because if an attacker manages to steal a plain text password file, the passwords of the server's user accounts can be easily swiped. The Australian Tax Office (ATO), The UK's Government Communications Headquarters (GCHQ) and retailer Tesco are all recent examples of companies that have been breached and subsequently admitted to storing their passwords in plain text.

2. **Basic Encryption:** This approach encrypts and stores an individual password (known as a "*hashed*" file). However, a stolen file that's been hashed once really isn't that much more secure than storing the password in plain text. Advances in CPU speeds and the availability of new password cracking software and both lookup and rainbow tables (precalculated tables of values that can be cross-referenced) means that it's only a matter of computing resources and time before most hashed password files are broken open.

3. **Random String Encryption:** This adds a random string to each password and then encrypts that value, which prevents an attacker from storing tables of precalculated values and looking for matches (this is known as a "*salted hash"*). Salted hashes aren't infallible, though: if the salt used is too short, or if the same salt has been used to salt all passwords, then it's possible to crack them open relatively easily.

4. **Multiple Encryption Passes:** This refers to the ability to encrypt an already encrypted value. The process, also referred to as "*stretching*," enables a value to be encrypted multiple times. However, there is much debate about whether this greatly improves security or not.

"Salted hashes and stretches are more secure than plain text or encrypted passwords for the time being," Henderson continued. "However, the ability to utilize the incredible power in today's CPUs means that it's likely just a matter of *when* and not if these types of encryption of passwords fall. Keep in mind that given enough time and resources, no type of password encryption is infallible."

Adding Another Factor of Authentication

Two–factor authentication, also referred to as multi-factor authentication, strong authentication and 2-step verification, consists of two of the following three methods of authentication:

- Something a user "knows:" This can be a password, challenge question or finger swipe movement over the face of a mobile device. This is commonly known as a *knowledge factor.*

- Something a user "has:" This can consist of a small hardware device, such as a smart card, USB key fob or a keychain dongle or a smartphone token, which generates a unique one-time password that's sent to or generated by an application on a user's mobile phone. This is known as a *possession factor.*

- Something a user "is:" This typically involves a biometric reader that detects something that validates something uniquely personal, such as a fingerprint, iris or voice. This type of authentication is known as an *inherence factor.*

The following user authentication options represent a few the most popular solutions available today along with a few of their pros and cons.

Passwords

The best thing about a password is that it's something a user knows or is easily remembered. It's the easiest (and least expensive) authentication option to implement from an IT perspective and a user doesn't need to possess an extra piece of hardware in their pocket or wallet. On the other hand, if a password is not complex enough, it can be easily guessed. If it's too complex, it could be forgotten. If a computer has been compromised with a botnet using a key logger, any password is easily swiped. Managing multiple passwords for multiple Websites is cumbersome. Software password crackers can crack simple passwords in minutes and cloud cracking services can crack complex passwords in a few hours.

Smart Cards

There are two types of smart cards (memory and microprocessor). The advantages of these cards are that their small, thin form factor makes them easy to carry around in a wallet or a pocket, and they can store a user's identity and PIN. The cons are that they require a reader on the computing device, those readers could conceivably be compromised, the cards must be issued and tracked, they can be easily lost, stolen or shared, they must be in a user's possession to access the computing device, it becomes locked after a number of bad attempts, and the card can break.

Fortinet's FortiToken-200 Provides Hardware-Based Authentication for Your Network

Hardware Tokens

Like smart cards, hardware tokens have many of the same pros and cons. Hardware tokens are more secure than passwords and more secure than smartphone tokens, as they're less susceptible to key logging hacks or other forms of malware designed to steal authentication credentials; they can be used for login and transaction authentication and users don't have to remember complex passwords. On the other hand, hardware tokens come at an additional cost (for the dongle itself as well as any additional software and hardware needed to manage the authentication), they must be in the possession of the user at login, multiple tokens may be required to access multiple Websites. Hardware tokens can be hacked though, as was the case with RSA's SecurID back in 2011.

Smartphone Tokens

Smartphone tokens are a lot like hardware tokens except that the authentication password is sent to or generated by an application on the user's mobile phone. The benefit to this approach is that a user doesn't need to carry around an extra piece of hardware in their wallet or pocket. Like hardware tokens, they're more secure than passwords, and there's no need for a user to remember complex passwords. However, like hardware tokens, smartphone tokens are not impenetrable against hackers. FortiGuard Labs has studied instances of the Zitmo Android botnet watching for two-factor authentication codes and sharing them with a command and control server.

Biometrics

There are two types of biometric user authentication: physiological includes fingerprint, facial, iris, retina and hand geometry scans and behavioral includes voice recognition, gates, keystroke/signature scans. The main advantage to biometric authentication is that authentication is coded to an individual, so there's no need to remember a complex password or carry another hardware device. On the other hand, these types of measurements are based on patterns and patterns hardly ever match precisely, which opens possibility for false positives and false negatives. A pattern recognition that is too lax could allow the wrong user into a system. One that's too strong could prevent a legitimate user from accessing a system.

Two-Factor Authentication Best Practices

Protecting sensitive data online by using multiple factors of authentication is the best policy for ensuring the safety and integrity of data. However, when matching authentication methods to your needs, don't assume that any two methods will work for your particular purpose.

It should be noted that, while two-factor authentication can offer greater protection, there are two types of attacks (masquerade and session hijacking) that can undermine any type of authentication. A masquerade attack is exactly what it sounds like: an attack that's able to assume a falsely-claimed digital identity and thus bypass the authentication mechanism. Session hijacking, also known as TCP session hijacking, happens when an attacker surreptitiously obtains a session ID and takes control of an already authenticated session. It's important to note that no two-factor authentication strategy can protect against a session hijack – ensuring all data is transmitted using SSL and HTTPS will help mitigate the chances of session hijacking taking place.

One important thing to keep in mind when planning out an authentication strategy: some types of two-factor authentication are stronger than others. In some cases, even a single factor may be inherently more secure than some two-factor implementations: a scan of the veins in a user's hands will be more secure than a simple password and one-time password card.

Before You Buy

Some factors you want to consider before purchasing a solution to implement two-factor authentication:

The tool's ease of use: How hard is it going to be to train your IT staff in its day-to-day operation? How much work will it take for initial setup and roll-out?

Integration with the existing software platform: will the solution "drop-in" into your existing infrastructure? Will any custom software development be required to integrate the solution?

Ability to meet security requirements/regulatory compliance: does your line of business or industry have any unique regulatory or reporting requirements that may require a certain type of implementation? Will choosing a specific solution meet those requirements?

The security of the tool itself: is the encryption algorithms used strong enough for your needs?

Vendor support: what sort of support or assistance can you expect from the developer of your solution?

Cost: what's the per-user cost to implement? Maintenance contracts? Additional costs to support the implementation at the Help Desk?

Future flexibility: will upgrades be available?

Two-factor authentication is an idea that is ready for wide-scale adoption. At FortiGuard, we believe the best way to keep a network and its users safe is to use technologies like two-factor authentication as part of a multi-layered security strategy. Adding two-factor authentication provides another layer of solid protection on top of any current security infrastructure.

Footnotes:

(1):http://www.prbuzz.com/technology/95904-new-research-on-two-factor-authentication-market.html

(2):http://www.marketsandmarkets.com/PressReleases/multi-factor-authentication.asp

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480