Guide to Evaluating Multi-Factor Authentication Solutions

Passwords are a known weak link and continue to be exploited at alarming rates. From simple phishing schemes to sophisticated, targeted phishing attacks, gaining access to a user’s password is an easy and prolific attack. Regulatory agencies agree and are setting increasingly rigorous requirements for strongly authenticating users. Multi-factor authentication is no longer optional for many organizations.

Whether you’re planning to implement multi-factor authentication for the first time or are looking to expand or upgrade your current implementation, this whitepaper will help you choose the solution that is right for your business. Key evaluation criteria will be defined and the most prevalent multi-factor authentication methods, including hardware tokens, smartcards, certificates, and PhoneFactor’s phone-based authentication will be evaluated against the criteria.

Contents

- What Is Multi-Factor Authentication 3
- Evaluation Criteria 3
  - Security & Stability 3
  - User Adoption 4
  - Total Cost of Ownership 4
- Hardware Tokens 5
- Smartcards 6
- Certificates 7
- PhoneFactor 8
- Conclusion 9
What Is Multi-Factor Authentication?

Multi-factor authentication combines any two of the following methods to strongly authenticate a user:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated)
- Something you are (biometrics)

In order to qualify as multi-factor authentication, two items must be combined from different categories, so a PIN plus a password doesn’t count as multi-factor, since both items are something you know.

Furthermore, the authentication is materially stronger when deployed across two different channels, that is, when it’s out-of-band. With out-of-band authentication, an attacker must compromise two networks to obtain access to a user’s account.

Evaluation Criteria

Evaluating multi-factor authentication solutions requires a look at three critical areas - the security and scalability of the technology, hurdles to user adoption, and the total cost (including internal costs) to deploy and support the system.

Security & Scalability

The underlying security of the authentication method is the most critical factor. If the second factor of authentication is not protecting your network, data, and users, then it’s not worth implementing at any cost. Given the ever-changing threat landscape, evaluating the level of protection is not an easy task. Industry experts and leading analyst firms are now recommending out-of-band or multi-channel authentication as a best practice. Also consider not just the threat prevention aspect of the solution, but also the threat alerting capabilities or other features that go beyond just stopping an attack.

As adoption of multi-factor authentication spreads to other areas of your business as well as among the companies you and your users do business with, interoperability will become increasingly important. It’s just not feasible for users to carry and keep track of multiple hardware tokens (i.e. one for work, one for their bank account, and one for their healthcare portal). Consider applicability with remote access platforms, intranets, customer websites and portals, email, point of sale applications, and payment systems.
User Adoption

User adoption is a key factor in the success of any multi-factor implementation. Users are resistant to changing their behavior and often see additional security processes as hindering their ability to get their job done. Users don’t want to carry an extra device, so they end up doing things like taping the token to their laptop which ultimately undermines the security of the system.

Another important element to consider is the portability of the system. BYOD is a trend that must be addressed in nearly every industry. Users want the freedom to login from any device, including home PCs, laptops and mobile phones, and to login from any location, including internet cafes, airport WI-FIs, remote offices, and client sites. The variety of devices and connection points can present significant challenges for IT departments, but the need for this level of flexibility will only increase going forward.

Total Cost of Ownership

Calculating the Total Cost of Ownership (TCO) for a solution can be difficult given the variance in implementation, deployment, and support costs. Internal costs can add as much as 30-50% to the total solution cost. These costs won’t show up on a purchase order from a vendor, so be sure to consider the following cost categories when determining the TCO:

- Hardware & Software
  - New hardware to set up and install
  - System integration (out-of-the-box versus custom)
- Deployment to Users
  - Cost of devices
  - Resources to provision and ship devices
  - End user training
- Device Maintenance and Replacement
  - Users lose and break security devices
  - Replacements must be shipped from the IT department
  - Without the device, the user can’t log in or has to bypass the second layer of security
  - Can result in significant hidden costs, user frustration, and lost productivity
- End User Support
  - Certificates installed on end user devices will need to be supported
  - Hardware tokens expire and have the potential to get out of sync
Hardware Tokens

Hardware tokens generate a pseudo-random sequence of digits referred to as a One-Time Password (OTP). The user is required to enter the OTP into the login screen to verify that they have possession of the token. While hardware tokens provide an additional level of security over single-factor authentication, they have proven to be cumbersome for IT departments and end users. In addition, more sophisticated threats have emerged that defeat hardware tokens.

Users are resistant to carrying an extra device, and as more companies implement multi-factor authentication, users could be required to carry several hardware tokens – one for their online bank account, one for their trading account, and one for their corporate vpn. Hardware tokens are easy to lose or break, creating a frustrating experience for users and placing a large burden on your IT department.

Because hardware token systems require users to change their behavior substantially, significant training is needed. When used in conjunction with a secret PIN, users sometimes have a hard time remembering which order the PIN and the token passcode are entered. The OTP is only valid for a short period of time, typically 30 or 60 seconds. So, users are in a constant race against the clock to key in the OTP before it changes. Some systems even require administrators to modify applications before they will work, evoking all of the change control difficulties associated with non-standard vendor software.

Since security tokens must be provisioned, mailed, inventoried, and replaced, they require significant IT resources to deploy and support. Hardware tokens are lost at a rate of up to 10% each year, expiring tokens must be re-provisioned every 2-5 years, and tokens can get out of sync, meaning the OTP that is generated is not the same one the login application is expecting. The resulting costs to an IT department can become a material part of the total cost of ownership for a token solution.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Multi-factor authentication across a single channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Adoption</td>
<td>Requires users to carry extra device(s)</td>
</tr>
<tr>
<td></td>
<td>Security tokens are easy to lose or break with no readily accessible alternative</td>
</tr>
<tr>
<td></td>
<td>End user training is required</td>
</tr>
<tr>
<td>Cost</td>
<td>Significant upfront authentication hardware/software investment plus cost for initial and replacement devices</td>
</tr>
<tr>
<td></td>
<td>High internal deployment and ongoing support costs</td>
</tr>
</tbody>
</table>
Smartcards

Another common two-factor solution involves the use of smartcards. Smartcards are credit card-sized tokens that have an embedded private key that is protected by a PIN or password. This private key positively identifies the user to the system.

Like tokens, users are required to carry around a new object that they didn’t have before. Cards must be provisioned, mailed, inventoried, replaced, and so on, creating similar logistical problems. And, since very few computers have built-in smartcard readers, an additional piece of hardware, including its drivers and associated platform dependencies, must be distributed to users and installed on the user’s computer. If that computer is compromised by malware, the data being passed through the card reader via the computer can be compromised as well.

Smartcards present lockout risks – most cards deactivate themselves after a certain number of failed attempts, and require physical replacement – leading to increased IT management time. In most cases, they require regular updating to stay current. Finally, few applications have native support for smartcard technology, and those that do often have narrow support for operating system versions, card reader models, and so on. Adding smartcard support to applications is often difficult.

While smartcards are effective when used to secure on premise access, their feasibility for remote use cases, mobile device access, and customer or public facing applications is limited.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Requires the use of smartcard readers and related drivers</th>
<th>Limited native integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Adoption</td>
<td>Requires users to carry an extra device</td>
<td>Access from mobile devices is likely not supported</td>
</tr>
<tr>
<td>Cost</td>
<td>Significant upfront authentication hardware/software investment</td>
<td>Cards and card readers must be purchased, deployed, and maintained</td>
</tr>
</tbody>
</table>

Certificates

Client certificates can be used as an additional layer of authentication, but are not a true second factor of authentication. A certificate is essentially a string of characters, which is installed on the end user’s computer.
Each certificate can only be used to authenticate one particular user because only that user’s computer has the corresponding and unique private key needed to complete the authentication process. Access is limited to the device(s) where a certificate is installed. Because the certificate is stored on the computer that the user is logging in from, it is trivial for malware running on the computer to copy and send it across the globe.

Client certificates are delivered electronically; however, deployment and support of digital certificates have proven problematic. This has been further exacerbated by the BYOD movement. Today, users are logging in from a wide range of desktop, laptop and tablet computers, as well as smartphones. So instead of managing a certificate on a single company-owned computer, IT departments must support multiple certificates per user across different devices and operating systems. In addition, allowing certificates to be installed on multiple devices degrades the security of the system.

Compatibility can be a major concern as well. There are a number of systems, including VPNs and other enterprise applications, which simply do not support the use of digital certificates. Interoperability with mobile devices is limited as well.

| Technology            | • Additional authentication, but not true two-factor  
|                       | • Easily defeated by malware                           
|                       | • Limited compatibility with applications and devices   |
| User Adoption         | • User must install a certificate on the device they are logging in from  
|                       | • Access from an unknown device is not supported        |
| Cost                  | • High implementation costs, then relatively low per user cost  
|                       | • Software set up and configuration                      
|                       | • High costs to support end users                       |

**PhoneFactor**

PhoneFactor combines the high degree of security that you need to protect your company from today’s attacks with a solution that’s easy to set up, maintain, and use. By leveraging something every user (employee, partner, and customer) already has, their phone, PhoneFactor works everywhere for everyone.

PhoneFactor offers multiple out-of-band methods (phone call, text message, and push) and an OATH passcode option, providing flexibility for users and a single multi-factor platform for IT to manage. Additional security features, like PIN mode, voiceprint, and transaction verification, can be mapped to particular users and/or levels of risk.
Because the PhoneFactor platform utilizes the telephone network for the second factor of authentication, it protects against all forms of malware, including keystroke loggers and man-in-the-middle attacks. Not only does PhoneFactor prevent unauthorized logins and transactions, it notifies you instantly if a user’s credentials have been compromised and an attack is in progress. By combining out-of-band authentication with real-time fraud alerts, PhoneFactor offers the strongest level of security on the market today.

With PhoneFactor there are no extra devices for users to carry and keep track of, and little end user training is required. The phone is an inherently user-friendly device and is accessible for users with disabilities. The same phone number can be used to authenticate any application, eliminating the need for multiple devices, and works anywhere in the world.

PhoneFactor secures access from all devices, including desktop and laptop computers, tablets, and smartphones, as well as access to the many applications (both on-premise and cloud) that require strong authentication.

Because there are no hardware tokens or other devices to deploy or manage, PhoneFactor requires very little effort to implement and virtually no ongoing support. PhoneFactor offers instant integration with all leading business systems and synchronizes with AD and LDAP servers for centralized user management. Easy, automated self-service options are available through the phone and web, which helps to significantly minimize overhead.

| Technology                   | • Out-of-band authentication options protect against malware threats |
|                             | • Real-time alerts notify IT of fraudulent activity               |
|                             | • Instant integration with leading enterprise applications        |
|                             | • Web plug-ins integrate with existing websites and online transaction processes |

| User Adoption                | • Easy authentication options (phone call, text message, and push to mobile app) |
|                             | • Works with any phone, anywhere                                      |
|                             | • No security tokens or extra devices to carry                        |
|                             | • No certificates to install                                         |
|                             | • User can log in from any device (smartphones, tablets, laptops, kiosks, etc.) |

| Cost                        | • Low annual fee per user or per auth                                |
|                             | • No hardware to purchase or install                                   |
|                             | • No security tokens or devices to manage                             |
|                             | • Users replace their own lost or damaged phones                        |
Conclusion

PhoneFactor combines strong out-of-band security with unparalleled ease of use for both users and IT departments, ultimately reducing the risk of a data breach at a lower total cost of ownership. As companies increasingly look to phone-based authentication to address today’s threats while also meeting the needs of growing numbers of enterprise and consumer users, PhoneFactor is the leading choice. PhoneFactor is trusted by thousands of organizations across virtually every industry, including Retail, Government, Healthcare, and Banking, to secure millions of logins and online transactions each month.

PhoneFactor was recognized in 2011, 2010, and 2008 as an SC Magazine Awards Finalist for Best Multi- and Second-Factor Solution and is a 2010 Network Products Guide Product Innovation Award winner. The company was also recognized with two Gartner reports, Cool Vendors in Identity & Access Management and Cool Vendors in Healthcare Providers. PhoneFactor has been named to the Bank Technology News FutureNow list of the top 10 technology innovators securing the banking industry today and recently earned a prestigious five stars in the SC Magazine multi-factor authentication group test.

For more information, contact PhoneFactor at 877.No.Token (877.668.6536) or visit our website at www.phonefactor.com.