MessageMedia
THE SMS SPECIALISTS

Balancing risk, cost and user experience with SMS for 2FA

MessageMedia Industry Intelligence

Contents

Security breaches are an increasing occurrence and a major issue for organizations. Compromise of internal systems and loss of proprietary and company and customer data can cause devastating financial, legal, and brand damage. Sony, Anthem, and Target are just a few examples of recent, high profile breaches. In many of these cases, hackers have used stolen or compromised user credentials to penetrate network defences.

Security experts have repeatedly pointed out the ineffectiveness of the traditional user name/password combination. A recent Ars Technica article[1] highlighted the ability of hackers to crack even seemingly secure passwords in a short amount of time. While so-called "strong" passwords offer a bit more protection, they remain vulnerable to increasingly sophisticated password cracking techniques (including social engineering techniques). Moreover, strong passwords are a challenge for users. Common practices for storing difficult to remember passwords often undermine the benefits of strong passwords. Meanwhile, forgotten passwords result in tedious password resets or users simply giving up.

System access via a simple user name and password is no longer enough because it is based on only one category of identifying credential; something you know. Two-factor authentication (2FA) provides additional security because it requires the user to provide two means of identification from separate categories of credentials; something you know e.g., a password and something you have such as a cell phone. The 2015 Verizon Data Breach Investigations Report listed 2FA as its number one recommended strategy for mitigating data breaches[2].

Security experts have repeatedly pointed out the ineffectiveness of the traditional user name/ password combination

Two-factor authentication (2FA) provides additional security because it requires the user to provide two means of identification from separate categories of credentials

1. ***http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/1/***
2. ***http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf)***

OTP Authentication Methods

One-time passwords (OTP) help to make the 2FA process even more secure because they are valid for only one login session or transaction. They are more secure than a static password, especially a user-created password, which is typically weak -- it requires knowledge and diligence to create and remember strong passwords.

There are different ways to make a user aware of the next OTP to use. The options available generally fall into two categories:

- Hard token-based solutions, which include key fobs and smart cards and
- 'Tokenless' or soft token methods such as mobile applications or biometrics. These soft methods leverage the devices, applications, and communications channels users already have. On-demand tokens may be considered a subset of soft tokens and include solutions that deliver OTP via SMS or email.

When considering the options for authentication methods, an organization must address three key areas: risk, cost, and user experience. Rather than choosing one method over another, it's all about selecting the optimal solution for users and the type of information that needs to be protected.

Advantages of SMS for OTP

Save money

Hard and soft token licenses cost $40-60 and have to be renewed every 3-5 years -- SMS requires only a one-time $20 ODA license.

Great ROI

A customer with 10,000 users could save over $500,000 (>150% ROI) in the first year by switching from hard tokens to SMS - use the MessageMedia ROI Calculator to estimate your own potential savings/ROI, visit ***http://www.message-media.com/roi-calculator***.

Improve user experience

Take advantage of the one thing your users already carry with them everywhere they go.

Enhance your security posture

Extending 2FA to 100% of your user base.

Hard Tokens for OTP

Token-based solutions have been around for decades and many companies still use them because they have implemented hard token infrastructure, deployed tokens and trained their users. Physical tokens may be a good OTP option for a company depending on its threat model, but they have a few drawbacks. The disadvantages of tokens typically include token handling, security and cost. For example, a typical RSA customer only rolls out tokens to 20% of users[1] because of the costs associated with a fob/token solution and the poor user experience often reported from token use.

Provisioning a hardware token to a remote worker involves setting the user up in a repository, assigning the token to a user and dispatching it. The dispatch process probably involves secured transit such as a registered mail service. This process takes time and the transit service alone could cost up to $50 per user, doubling the cost of the hardware token itself. If employees are based all over the world, additional costs are incurred sending the devices to them.

The issue of lost or stolen tokens is also considerable. Surveys indicate that an organization with 600 users would typically expect up to 10 tokens lost per month, equating to 1.67% of the installed base. If the hardware token costs $50 and it costs an additional $50 to dispatch the token then the cost of handling lost tokens alone can add a cost of $1000 per month which should also be factored in to any solution costs.

User experience is also an issue. A user is reliant on the token and has to carry it with them at all times for authentication. If a token is lost or forgotten, access is not possible. Users are increasingly reluctant to carry a key fob with them, in addition to cell phone, keys, wallet, etc. Senior executives, who typically have high-level access, are often the least willing to carry a key fob.

Also, tokens are easily lost or misplaced, which at a minimum introduces additional admin overhead including token replacement costs. This also represents a security risk as the fob could be stolen and used by someone else without the end user noticing that it was missing.

1. ***http://www.emc.com/collateral/rsa/auth8-infographic.pdf***

App-based tokens for OTP

The driving force behind the update of software tokens is the growing penetration of smart phones that are capable of running apps.

The explosion in apps for business use presents a problem for authentication when using a token app on the same device. If you're using apps on your smart phone to access corporate data and rely on another app on the same device to be the 'something you have', is that really two-factor authentication? Moreover, some users may push back on the requirement to have to download yet another app.

App-based tokens may also impact business overhead due to admin costs associated with supporting and troubleshooting issues with the app. In a BYOD environment, organizations have to be cognizant that not all users own a smart phone. Even those that do own a smart phone may not use a model or O/S that is supported for the app.

App-based tokens have significant drawbacks in scenarios involving contractors or partners, as well as business continuity use cases. For users, such as contractors, who authenticate infrequently, the cost of the app license and the requirement to download the app may not be practical. Moreover, app-based tokens are typically not extensible, meaning that they will be a challenge for third party users who have to authenticate to multiple systems. Finally, app-based tokens are not suitable for business continuity and disaster recovery scenarios, in which a solution has to be deployed quickly and unexpectedly to a large number of users.

Email vs. SMS for OTP

Email for OTP

OTP can be delivered to users by email, however this is not an out-of-band solution. The OTP is being delivered over the same channel that the user uses to authenticate and access the network. As such, OTP via email is essentially single-factor authentication. Moreover, email accounts are typically protected with only user name and password, which means that they are themselves relatively easily hacked. It's also relatively easy to forge or spoof an email.

From a user experience perspective, email has at least two drawbacks. First, email delivery delays or failures result in user frustration and inability to log in. Second, the user may be trying to log into an email account that requires 2FA. If the OTP is delivered via email to the email account in question, the user won't be able to access the OTP and thus won't be able to log in to the email account.

SMS for OTP

SMS is a tokenless 2FA solution that provides all the security functions of hardware tokens with no need for additional hardware. It means that BYOD immediately becomes BYOT: 'bring-your-own-token'.

Aspects such as deployment, manageability and superior authentication are just a few things that set SMS-based authentication apart.

SMS also makes sense because it is a less expensive method that is easy to use and requires no user training, as virtually everyone knows how to send and receive an SMS.

Using a unique SMS code to confirm identity is remarkably efficient. The message is sent in seconds and when you work with a reputable service provider, the message will arrive at a user handset almost immediately.

Benefits

Business Benefits of SMS

- Maintains anywhere, anytime access;
- Inexpensive, and lower deployment costs. No hard or soft token licenses are required and On-demand Authentication (ODA) licenses are cheaper (~$20) than hard or soft tokens ($40-60) and, unlike hard and soft token licenses, they never expire;
- Reduced on-going administration. Companies don't have to issue, track, retire, ship or replace tokens. SMS also reduces support desk costs related to lost/misplaced key fobs, or issues with soft token apps;
- Ideal for anyone with a one-time or infrequent need for 2FA such as part-time or temporary employees, contractors, vendors or customers;
- Can be distributed immediately;
- Works with a variety of applications including VPN, web portal and Citrix;
- Device and OS independent; provides a standard delivery platform for authentication by working with any standard mobile phone on the market today.

User Benefits of SMS-based Authentication

- Most people have a phone capable of SMS and carry it with them;
- SMS is easy to manage and virtually everyone knows how to use it;
- Requires no hardware distribution or software installation to the end user's mobile device.

Security of SMS

Each OTP methodology has its strengths and weaknesses. Token-based solutions can be vulnerable as a hardware token has a fixed algorithm that may be compromised and reproduced without the user ever knowing. However, an SMS pass code doesn't have to follow any predictable algorithm; the code can be completely random. And if a seed file and/or algorithm is compromised it is far easier to change the SMS OTP seed file and algorithm rather than a fleet of hard tokens.

Other security measures are available for SMS such as event-based or time-based pass codes. Options include setting codes to expire after a few minutes or even seconds, the ability to send the next code immediately after the last one is used, "day use" codes or multiple codes in each SMS.

SMS pass codes may also have some benefits when it comes to repudiation (or non-repudiation) because the physical location of a mobile phone is tracked and it's possible to investigate user activity and correlate it with a particular login.

On the provider side, reputable SMS companies use VPN connections and other best practice security measures to ensure secure transmission of encrypted messages from customer systems to the carrier networks.

SMS also has a security benefit in that users are far more likely to notice a missing cell rather than a missing token.

And lower costs and admin overheads means that organizations can deploy 2FA to a greater percentage of their users, which translates into increased security for the organization by reducing or even eliminating 'weak links'.

How SMS Fits Into a Broader 2FA Roll Out

Organizations that have implemented hard token solutions may be understandably resistant to swapping out the entire solution for a soft token option. However a hybrid approach using a combination of hard and soft tokens, in particular SMS, can be implemented with relative ease.

Many organizations chose to replace hard tokens and app-based soft tokens on a rolling basis as token licenses come up for renewal.

A common approach for organizations is to start with a small proof of concept deployment of SMS for OTP. Once the proof of concept has demonstrated the cost, administrative and user experience advantages of SMS, existing tokens are replaced with SMS en masse or on a rolling basis.

As for new 2FA implementations, founder and managing director of Goode Intelligence, Alan Goode said that they have seen a steady rise in the adoption of mobile devices as two-factor authenticators estimating that it probably accounts for over 20% of total 2FA sales.

SMS is appropriate:

a. As replacement for hard/soft tokens

b. As supplement to existing hard/soft token deployment (i.e., expanding 2FA to other users not currently secured by 2FA):

i. Other employees
ii. Contractors
iii. Suppliers/partners/customers

c. For business continuity – e.g., if your employees suddenly and unexpectedly have to work from home due to a disaster or otherwise. With SMS, you can easily deploy 2FA to thousands of users; RSA even offers a Business Continuity option that gives you the ability to instantly issue up to 10K On Demand Authentication licenses.

There are a few scenarios in which SMS may not appropriate. For example, SMS delivery won't work in underground or remote facilities with no cell coverage. Likewise, SMS is not suitable for facilities in which cell phones are not permitted.

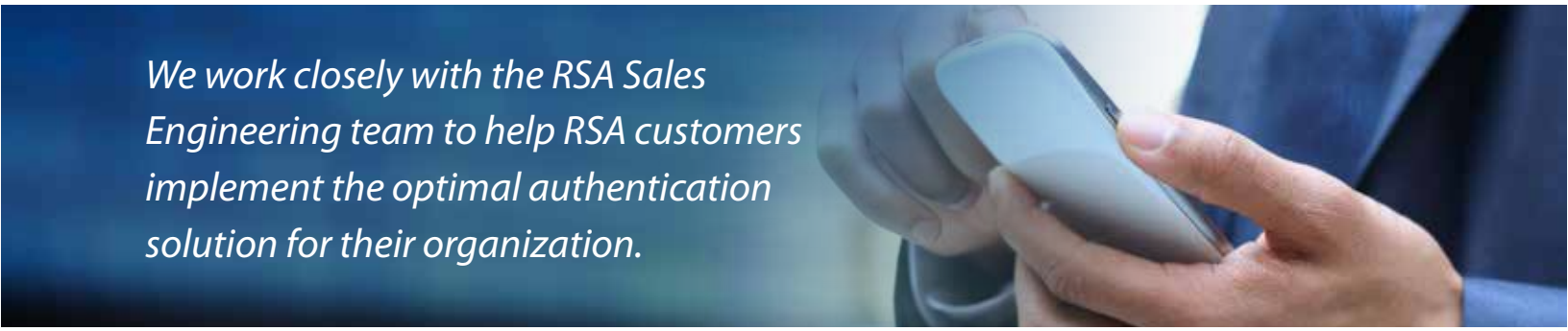
Implementing RSA SecurID with SMS

RSA is the premier provider of intelligence-driven security solutions and helps the world's leading organizations solve their most complex and sensitive security challenges.

RSA SecurID On-demand Authenticator delivers an OTP to a user's mobile device via an SMS text message or email, turning that mobile device into a security token. This gives mobile users a constantly changing, secure, two-factor authentication password to protect access to sensitive applications.

a. If you're an RSA customer – contact MessageMedia or your RSA Sales Engineer; you can be up and running with SMS for your existing Authentication Manager deployment in minutes

b. If you're not an RSA customer – contact MessageMedia to discuss options for integrating SMS with your existing 2FA solution; we work with both customer proprietary solutions, as well as other 3rd party solutions



How MessageMedia Can Help

MessageMedia is a member of the RSA Ready Technology Partner Program and has significant experience with the RSA Authentication Manager and SecurID Authentication technology. We work closely with the RSA Sales Engineering team to help RSA customers implement the optimal authentication solution for their organization.

Beyond RSA, MessageMedia has experience working with customers across a wide range of industries. Our recent 2FA experience includes the deployment of SMS for OTP to one of the leading securities exchanges, the number #1 ranked hospital network, a Fortune 100 retailer, a top 5 energy company, a leading media conglomerate, and one of the largest healthcare companies in the world.

MessageMedia delivers unparalleled service reliability and industry leading customer support.

Our gateway platform is designed to deliver carrier-grade redundancy, featuring multiple, redundant network connections and SMS routes. The gateway is monitored 24/7 by a heart beating system, and dynamic message routing means that in the event an SMS gateway goes down, outbound messaging is automatically redirected to an available gateway, so the message gets through. We also prioritize processing of OTP messages to ensure the fastest possible delivery.

This is a critical time-sensitive service, so you need help on hand when your business and customers need it, and you shouldn't have to pay extra for that level of service, it should come as a standard. With global offices, MessageMedia offers a follow the sun customer support model, which means customer calls are answered 24/7.

TECHNOLOGY RSA READY PARTNER

Why MessageMedia?

Reliability
99.7% of messages are delivered in 30 seconds

Speed of Deployment
Be up and running in minutes, rather than weeks or months

Support
Live, 24 x 5 support with optional 24 x 7 coverage

Reach
Delivery to over 200 countries worldwide

Experience
Over 15 years' experience and more than 15,000 customers organizations in financial services, healthcare, technology, and government

AUSTRALIA
Level 22
385 Bourke Street
Melbourne VIC 3000
T: 1800 009 767
E: sales@MessageMedia.com.au
www.MessageMedia.com.au

UK
Level 6
52 Grosvenor Gardens
Victoria London SW1W 0AU
T: 0808 234 8246
E: sales@MessageMedia.co.uk
www.MessageMedia.co.uk

USA
Level 5
One Embarcadero Center
San Francisco CA 94111
T: 888-799-9767
E: sales@Message-Media.com
www.Message-Media.com

MessageMedia
THE SMS SPECIALISTS

Copyright © 2015 MessageMedia