What You Need to Know About the Security of SMS and Two-Factor Authentication
Examining the Arguments for and Against This Methodology
Table of Contents

4  Introduction
5  Examining Common Arguments Against 2FA over SMS
9  Summary
For the vast majority of applications that require the extra security that two-factor authentication (2FA) provides, in the vast majority of situations, SMS will more than suffice as a delivery channel. Most enterprises and end users can view 2FA over SMS with confidence as a key method of providing security. In this paper we address recent arguments about the efficacy of this delivery methodology and examine what you should know about 2FA leveraging SMS going forward.
Two-factor authentication (2FA) is one of the most effective ways of protecting accounts, and it is widely used across the world. A common and convenient method of deploying 2FA is to deliver tokens (PIN codes, verification codes, one-time passwords, and the like) through SMS to the user’s mobile device.

In a survey performed in 2016 by the SAP® Digital Interconnect group (formerly SAP Mobile Services), 75% of the respondents indicated that SMS was their preferred delivery methodology. Furthermore, 85% of the respondents said they preferred receiving an authentication code on their mobile device to provide additional security with their user ID and password for online transactions.

As an out-of-band delivery channel, SMS is overwhelmingly popular with consumers and is provided by major online shopping sites such as Amazon and eBay as well as banks, social networks, e-mail providers, and many others. The key benefit to SMS is that users don’t need to download a specific mobile, code-generator, or authenticator app, which could be viewed as a barrier to 2FA adoption by consumers.

In June 2016, the United States National Institute of Standards and Technology (NIST) published a draft of its Digital Identity Guidelines (NIST SP 800-63-3). Section 5.1.3.2 noted that out-of-band verification through SMS will be deprecated and will not appear in future releases of NIST’s guidance. This recommendation is specifically targeted for U.S. government applications.

The NIST proposal raised significant alarm in the United States and elsewhere about 2FA over SMS, evidenced by some attention-grabbing headlines proclaiming that the end of 2FA through SMS was at hand. This sort of exaggerated hype is damaging to 2FA overall. Furthermore, while the NIST recommendations do bring up valid points, we believe that most of them are of debatable value because they represent rare edge cases, and if followed would unnecessarily limit use of 2FA — which remains a very good solution that benefits overall security for the majority of situations.
Arguments against 2FA over SMS as an out-of-band delivery channel range from SIM swap fraud to issues with encryption to questions about the availability and efficacy of SMS itself. Let’s examine a few of these.

**INTERCEPTION OF A PHONE NUMBER (SIM SWAP FRAUD)**
There have been a number of attacks against mobile phone providers in which the attacker transfers the phone number to a third party. This is called SIM swap fraud (for background, see this [UK-operator-centric post](#)). This fraud requires a bit of social engineering by attackers on the mobile operator representatives. The fraudsters must convince whoever they are dealing with at the mobile operator that they are, in fact, the owner of the phone number. If this happens, it can be serious and difficult to overcome.

Today, solutions vary by country, but most major operators around the world have already put in protections against this type of fraud or are in the process of doing so. For example, in the United States, mobile operator reps ask for a particular security passcode that subscribers have set before any action will be performed on the account through a chat or phone call. This is different from the account password. Other operators (such as O2 in the article mentioned above) provide an SMS validation code to the current device.

While SIM swap fraud does still occur in some markets, it has become rarer as mobile operators are implementing new security procedures and protocols for customer service reps to prevent this type of fraud. For most applications, the potential security issue of delivering 2FA tokens to phones via SMS does not outweigh the benefits and convenience of 2FA over SMS.

For most applications, the potential security issue of delivering 2FA tokens to phones via SMS does not outweigh the benefits and convenience of 2FA over SMS.
**INTERCEPTION ON THE DEVICE**

Some devices may be compromised by malicious apps that can intercept SMS messages and relay the content to bad-actor third parties. In these cases, the user of the device has likely been deceived through some social engineering technique into accessing the malicious app through a nonstandard app store or by downloading unknown or phishing data from an e-mail – both practices that are fraught with peril anyway.

Yes, this can be done; however, in these cases, we need to assume that device owners should maintain some control over what is downloaded to their device. Legitimate Android and Apple app stores actually have very little (known) malware. While it could be possible that what appears to be a legit app can have malicious capabilities, these cases are rare.

Again, limiting or deprecating 2FA over SMS as a result of these types of situations is significant overkill. With some malware, time-based one-time password (TOTP)—compatible authenticator apps may be equally compromised through the use of screen-scraping technology.

Overall, these very technical arguments against SMS are definitely not wrong, but in real-world cases, they relate to situations that are already quite rare and are diminishing in frequency. It is easy to cite SIM fraud or SMS interception as an argument against 2FA over SMS, but even so, two-factor authentication is just that – **two** factors – the first being a user ID/password (something the user knows) and the second being the delivered verification code via SMS. So unless the bad actors have both factors, the account is still protected.

**ENCRYPTION QUESTIONS**

This issue is related to the 2G GSM standard, which uses an over-the-air encryption scheme called A5/1. There have been a number of published attacks on A5/1, and it can be decrypted in real or near-real time. In fact, documents leaked by Edward Snowden in 2013 indicate that the U.S. National Security Agency can process encrypted GSM A5/1.

2G is still in use, but many operators are already shutting it down or have announced plans to do so in 2017. A primary reason is that mobile network operators need to repurpose the 2G radio frequency bands for Long-Term Evolution (LTE) and beyond. This leaves 3G and LTE to support basic services such as voice and SMS – both of which employ much more robust over-the-air encryption.

It has been said that 2G towers are easy to spoof and the encryption is easy to break, and that most phones will downgrade (from 3G or LTE) without informing the user. The downgrading part is true; however, most actors that can deploy or spoof 2G fake towers are extremely sophisticated, and the cost versus the benefit of doing this to capture 2FA over SMS messages is limited at best. Consequently, this is an edge-case risk. But again, while the decryption is certainly possible, it is not practical and definitely is not a reason to rule out 2FA over SMS for most applications.
SMS RELIABILITY AND EFFICACY

Detractors of 2FA over SMS will cite SMS reliability as an argument against using SMS as an out-of-band delivery channel. They will say that 2FA codes should have a short (typically less than 15 minutes) expiration time. We say, the shorter the better, but not so short as to not be useful – a 10- to 15-minute range is quite sufficient.

SMS delivery times are highly dependent on how messages are delivered. While the details are sometimes complex, it is incumbent upon the business that offers 2FA over SMS to use a well-known and respected SMS provider. SMS reliability is absolutely dependent upon how messages are routed from the enterprise entity to the appropriate mobile operator.

Service providers that offer lower-cost or least-cost routing for 2FA traffic (for example, by leveraging the so-called grey routes for SMS) run the risk of having their messages delayed or blocked entirely. SMS delivery providers who employ hundreds or thousands of originating numbers in an attempt to avoid message blocking on behalf of their customer (for example, a bank), are usually trying to get around regulations.

The SMS delivery provider should leverage as many direct mobile operator connections as possible, using all high-quality routes since many of these 2FA tokens have short expiration times. It is imperative that these SMS messages comply with all regulations and best practices for the country and mobile operator for which they are intended. When they do, the message delivery rate is extremely good and usually occurs within seconds.

Another common argument against SMS for 2FA is that some locations don’t have phone reception, either due to their location or because the user is in a different territory with an incompatible phone device or without roaming enabled. Lack of mobile phone reception (such as within some buildings) can be an issue for some people. To overcome those situations, an enterprise deploying 2FA should consider multiple delivery channel options – for example, the 2FA token could be delivered to an e-mail address, accessible from a connected laptop. Alternatively, the enterprise could also use validation of tokens generated by a specialized authentication app such as Google Authenticator to support those users who don’t have indoor (or even roaming) connectivity. Once again, while these edge cases do exist, they do not amount to a reason to completely abandon 2FA over SMS for the majority of users.

SMS is limited to a single device because it is tied to the user’s phone number, while a TOTP app can be used on multiple devices such as a mobile device and a desktop. This is actually not a bad situation. In today’s mobile age, the mobile device is almost always with its owner. The single phone number acts as a true out-of-band address – a good thing for using 2FA with SMS as the delivery channel.
HIGHER LEVELS OF PROTECTION
There are situations in which an enterprise may not want to expose its customers to the risk, however small, of receiving an authorization code through SMS – for example, for high-value financial transactions or access to government or high-security applications or platforms. In these cases, the recommendations put forth in the NIST guidelines can certainly be valuable.

For many users, a TOTP-based authentication app (such as Google Authenticator) on their mobile device provides incrementally more security than receiving the authentication or verification code via SMS. TOTP apps are relatively easy to download and use on smartphones and typically do not require a data connection to generate a code. The app must be configured to work with the site or application by the user (or IT department). However, this is typically trivial – although there could be issues with changing or upgrading devices, according to feedback on various apps.

If a user’s mobile device is questionable, then high-security options include using separate hardware tokens or deploying three (or more) factors such as biometrics (fingerprint, iris or retina scan, facial recognition, or voiceprint).

In very nearly all situations, 2FA over SMS provides sufficient security to protect both enterprises and end users from fraud, with little disruption for the end user.
What You Need to Know About the Security of SMS and Two-Factor Authentication

Summary

For most applications that need the extra security that two-factor authentication provides, SMS as a delivery channel will more than suffice in most situations. While SMS may not be completely secure since the messages are transmitted over mobile networks, this is still a high-security solution. We should note that 2FA tokens generally have a short expiration time – usually no more than a few minutes – and that there are limitations on how many times a user may try to enter a received code before the solution locks the user out for a specific time period. While no scheme is 100% secure, in very nearly all situations, 2FA over SMS provides sufficient security to protect both enterprises and end users from fraud, with little disruption for the end user. Add to this the fact that it is convenient and does not require any additional downloads or app installations, and you have a solid and practical security solution for most uses.

TO LEARN MORE

The SAP® Digital Interconnect group offers a global, reliable messaging aggregator using SAP SMS 365, enterprise service, as our messaging hub. SAP Authentication 365, a mobile service, is an end-to-end, portable, and configurable 2FA solution for multiple channels including SMS, push notifications, and e-mail through the SAP Intelligent Notification 365 mobile service, URL validation via SMS, and more. SAP Authentication 365 provides:

• Integrated connectivity to SAP SMS 365, enterprise service, connects with more than 1,000 mobile networks through a single, standard interface
• Accurate and fast message routing using our advanced number resolution system to correctly identify the destination mobile network operator
• High-priority messaging delivery solutions to ensure fast delivery of 2FA/OTP messages
• Highest-quality approved routes for delivery of all messaging, including 2FA/OTP messages
• Multiple configurability options for 2FA tokens as well as a comprehensive administrative and analytics user interface
• Simple, secure application programming interfaces (APIs) for easy integration of 2FA capabilities into existing workflows

For more information, contact your SAP representative or visit www.sap.com/product/technology-platform/enterprise-sms-authentication.html.