Is SMS Secure?

An examination of the security risks with SMS technologies with MFA and security applications

SecurEnvoy
A Shearwater Group plc Company

Security Beyond Boundaries.

Is SMS Secure?

The security of SMS has always been a concern for industry, businesses and individuals alike since 1992, when the first message was sent. Now, over twenty years later, SMS has seen tremendous growth, with 7 billion SMS messages being sent in 2017.

SMS is an integral part of our digital lives. We interact on a number of occasions from simple messaging, to appointment booking/reminder to transaction alerting and secure authentication. User authentication has been widely used for e-commerce from a user engagement of sending a temporary key or password to gain access, to more evolved systems such as Second Factor Authentication (2FA).

The key to using SMS for MFA is "trust." The user has their assigned GSM mobile device, of which they provide personal protection around, the e-commerce site would then trust this interaction and can provide the additional security of sending a key (passcode or password) via SMS, of which the recipient responds, and validation occurs. 2FA systems had additional security measures in place, such as only sending the key once a previous authentication had occurred (2FA), sending a time limited key (passcode or password), monitoring and blocking attempts to re-use a previously used key.

The major benefit to SMS was that security was provided by the TELCO provider via standards in the GSM protocol and the end user only had to register to use any service with their subscriber ID (mobile number) - no software to install update or manage.

A Historical View

Businesses then saw SMS MFA as a way to help detect and respond against fraud attacks for their online users, especially for e-commerce and finance. However, it wasn't long before compromises were seen in the public domain. Namely rogue Telco staff accessing log data to see message transfer data (insider threat), to Telco staff creating a cloned sim. A number of cases were seen in South Africa where internal staff used duplicate SIM's to commit fraud. Telco's now have controls in place to detect duplicate connections and drop the from the network in real time. As for the insider threat, this is still a real concern, knowing who is policing the Telco. Telco's have put a lot of effort into removing rogue employees, namely anomaly detection of staff, access controls, threat metrics and other counter measures. As any breach is damaging and provides loss of branding and reputation.

Like all things in life, everything evolved, the bad guys then tried to attack the wireless network and intercept traffic between the mobile device and the telco network. Encryption is used for the wireless connection between the GSM handset and the SMS Service Centre. There were attacks on this vector, where data and voice were compromised, but SMS used the signalling channel so wasn't so open to this technique. The algorithm's utilised were then strengthened to provide additional resistance. It was at this point that Smart phone technology was prevalent, this then provided the ability to infect the phone with a trojan to forward any SMS to another mobile identity, all this occurred silently to the user. The bad guys were now directly attacking the end user rather than the Telco network, as this allowed easier attacks to be escalated. The scenario would be to obtain user account records from the Dark Web, then carry out a phishing attack to fish other personal information and or passwords. The last part would be to infect the user's phone (trojan) to obtain the key set via SMS to allow access or approve a rogue financial transaction.

This game of cat and mouse continued and two things then occurred: namely security, malware and AV protection for smart phone devices. 2FA operators started to use PDU mode instead of text mode for SMS which allowed an SMS to go directly to the phone screen, thereby bypassing the SMS inbox.

At this point in time, attacks were being seen against the GSM wireless vector. A rogue base station was presented in a targeted area of which the GSM mobile would connect to as this was seen to have the strongest signal. As no encryption key was exchanged, all traffic was in the clear. This approach required skill plus costly hardware, as this was effectively a man in the middle (MITM) attack on the GSM network. The Telco community responded by having the ability to detect and kill of these rogue points, plus they hardened the mobile device to only to connect to the actual service provider 02, EE, Vodafone, AT&T etc.

The REDDIT Debacle

Now in the latest news there is an article regarding REDDIT. The SMS keys were compromised to access their systems. This raises a number of points of concern, firstly, did they only rely upon the SMS key along with a User ID to for access? As they describe quote “strong authentication requiring two factor authentication (2FA)”. But what they do not explain, is that to conduct this attack, a prior phishing or credential highjacking attack to obtain the User ID’s and passwords had already occurred. Or had these details already been compromised and on sites such as paste bin or were being sold on the dark web? I’ll guess we will never know.

REDDIT talks about SMS interception, yet provides no further details upon this. There are three types of attacks that could meet this scenario, and will go through each one in turn of what could be accomplished.

First and the easiest scenario, a bad guy sends you an SMS that looks as though it has come from a friend or service asking for monies or your login details. This can be achieved by using a rogue SMS Service Centre (SMSC), as the GSM protocol provides a clear boundary of protection, but when you’re seen on the inside there is little or no security. This allows the sending of a masqueraded message to trick you into doing something or providing other information, as the message is not authenticated or validated.

Second is the next hardest step for an inception attack. The GSM network only authenticates the phone when connecting. The network never authenticates itself to the user mobile phone (mutual authentication). To conduct this, you must set yourself up as a rogue base station, broadcast the correct Country and Network identifiers and hey presto you have mobile subscribers connecting. These attacks are always limited by geography. So, the bad guys will have to be specific on where the end users are to target.

The third scenario is ultimately the hardest and requires a lot of skill and equipment. This is where the authentication key code of the mobile must be cracked. To complete this task requires complex hardware to monitor the same wireless spectrum as the targets mobile phone. Once enough phone registration data is obtained reverse engineering of the authentication key can be achieved. But this requires at least multiple days of recorded traffic to complete. Finally, once the key has been compromised. Must wait for the targets mobile device to be idle, before the bad guy can attempt to connect and register to the Telco network.

The Great Bitcoin Heist

In February of this year, T-Mobile sent a mass text warning customers of an “industry-wide” threat. The threat they were referring to is known as SIM Swapping or SIM hijacking. In previous years to mitigate this, T-Mobile and other carriers introduced PINs or security passwords required in order to make any account-based changes. Even these efforts could be circumvented by rogue agents who might find a sympathetic ear with a customer service agent. In the case of the Bitcoin theft ring that was uncovered in Michigan this year, they went direct to the source and had paid contacts at the cellular company to activate a SIM swap on their behalf. Once the ring identified targets with large amounts of Bitcoin, they worked to identify their carrier and execute the SIM swap to execute the theft. They moved the Bitcoin to other accounts and used ATMs across the United States to withdraw cash.

SMS for Security

There are issues with SMS, but when relying on good security and best practises, SMS still does have a prominent place at the table. It is still better than just a password only approach. In fact, many of the detractors will spend paragraphs railing against the use of SMS, but then offer the caveat that it's better than nothing at all.

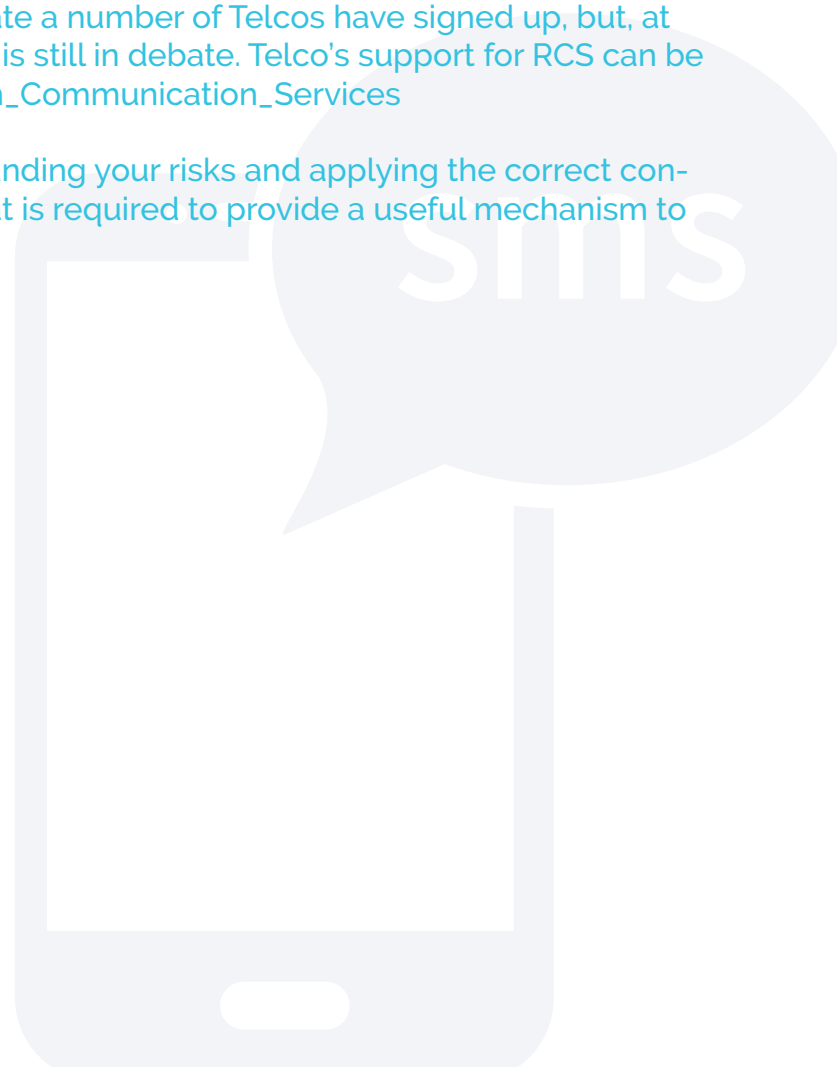
Additionally, it's important to remember the efforts rogue agents must go through to intercept or acquire SMS messages. The barriers are so high that the most common occurrences are against specific targets, not the public at large. Where password attacks can target millions at a time, most SMS attacks are against specific individuals for specific reasons such as owning high value Instagram account names, owning large amounts of Bitcoin, etc. Companies such as Paypal, Microsoft Cloud and certain banks still use SMS.

One comment that did raise an eyebrow is the comment from REDDIT to use only an authenticator app, aka soft token. If the authenticator app has an application program interface (API), a targeted trojan can interrogate this to obtain passcodes. This is especially true for time synchronous tokens, where the passcode and time stamp of when it is valid is obtained. How many authenticator apps split the core algorithm to generate passcode information (a SEED record) thereby providing additional protection from copying or compromise?

Yet again a game of cat and mouse and security escalation continues. From the industry on all sides updates are provided to their mechanisms, more detailed counter measures will be deployed and additional monitoring tactics offered.

Telcos are now looking to implement RCS which will be the second generation of SMS. This is to be fully ratified as a GSM standard. To date a number of Telcos have signed up, but, at this time end to end encryption of messages is still in debate. Telco's support for RCS can be seen here https://en.wikipedia.org/wiki/Rich_Communication_Services

A mixture of security best practises, understanding your risks and applying the correct context of correct security and monitoring is what is required to provide a useful mechanism to authenticate your users.



Our Global Team

Let's Talk.

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 (0) 89 44 47 92 00

Level 40 100 Miller Street
North Sydney
NSW 2060

General Information

E info@SecurEnvoy.com
T +612 9911 7778

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211