How hackers can use message mirroring apps to see all your SMS texts and bypass 2FA security

August 16 2021, by Syed Wajid Ali Shah, Jongkil Jay Jeong, Robin Doss

Credit: AI-generated image (disclaimer)

It's now well known that usernames and passwords aren't enough to securely access online services. A recent study highlighted more than 80% of all hacking-related breaches happen due to compromised and weak credentials, with three billion username/password combinations

stolen in 2016 alone.

As such, the implementation of two-factor authentication (2FA) has become a necessity. Generally, 2FA aims to provide an additional layer of security to the relatively vulnerable username/password system.

It works too. Figures suggest users who enabled 2FA ended up blocking about 99.9% of automated attacks.

But as with any good cybersecurity solution, attackers can quickly come up with ways to circumvent it. They can bypass 2FA through the one-time codes sent as an SMS to a user's smartphone.

Yet many critical online services in Australia still use SMS-based one-time codes, including myGov and the Big 4 banks: ANZ, Commonwealth Bank, NAB and Westpac.

So what's the problem with SMS?

Major vendors such as Microsoft have urged users to abandon 2FA solutions that leverage SMS and voice calls. This is because SMS is renowned for having infamously poor security, leaving it open to a host of different attacks.

For example, SIM swapping has been demonstrated as a way to circumvent 2FA. SIM swapping involves an attacker convincing a victims's mobile service provider they themselves are the victim, and then requesting the victim's phone number be switched to a device of their choice.

SMS-based one-time codes are also shown to be compromised through readily available tools such as Modlishka by leveraging a technique called reverse proxy. This facilitates communication between the victim

and a service being impersonated.

So in the case of Modlishka, it will intercept communication between a genuine service and a victim and will track and record the victims's interactions with the service, including any login credentials they may use).

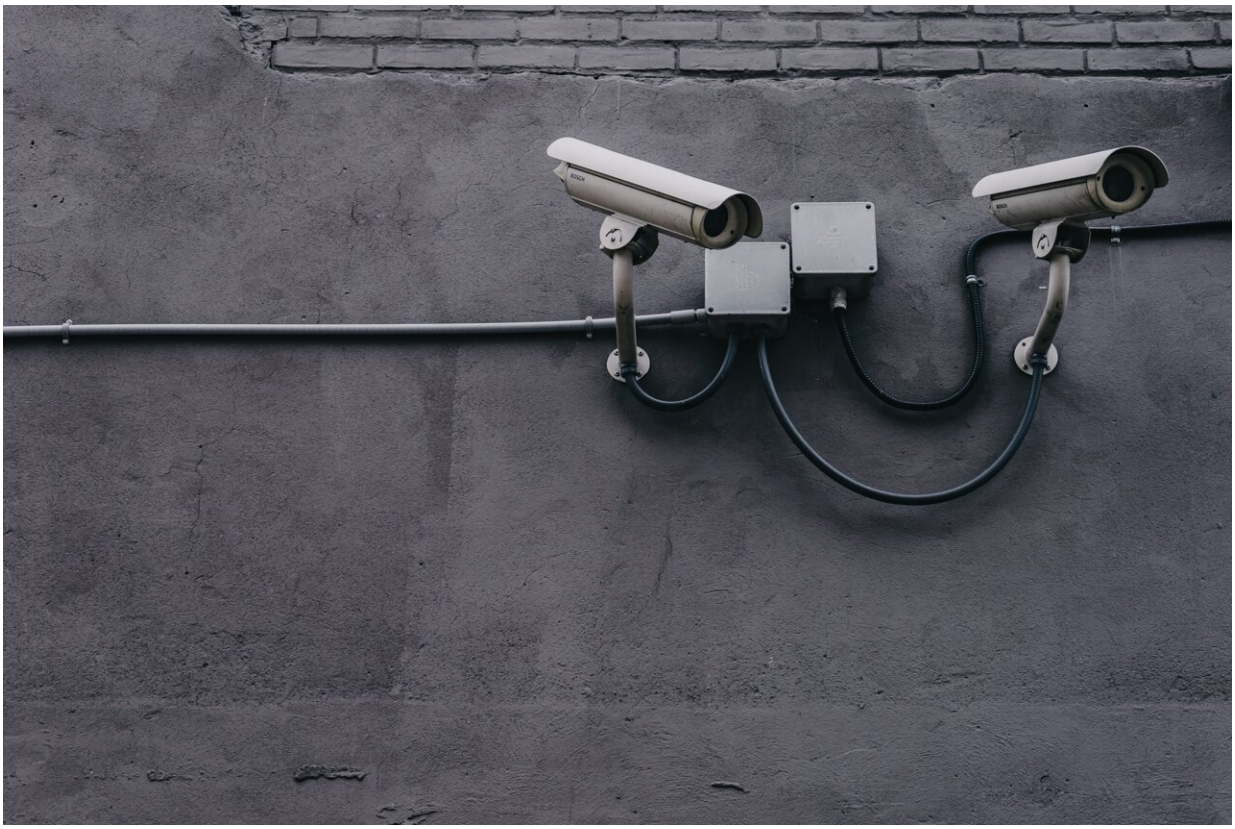
In addition to these existing vulnerabilities, our team have found additional vulnerabilities in SMS-based 2FA. One particular attack exploits a feature provided on the Google Play Store to automatically install apps from the web to your android device.

If an attacker has access to your credentials and manages to log into your Google Play account on a laptop (although you will receive a prompt), they can then install any app they'd like automatically onto your smartphone.

The attack on Android

Our experiments revealed a malicious actor can remotely access a user's SMS-based 2FA with little effort, through the use of a popular app (name and type withheld for security reasons) designed to synchronize user's notifications across different devices.

Specifically, attackers can leverage a compromised email/password combination connected to a Google account (such as username@gmail.com) to nefariously install a readily-available message mirroring app on a victim's smartphone via Google Play.



Credit: Unsplash/CC0 Public Domain

This is a realistic scenario since it's common for users to use the same credentials across a variety of services. Using a password manager is an effective way to make your first line of authentication—your username/password login—more secure.

Once the app is installed, the attacker can apply simple social engineering techniques to convince the user to enable the permissions required for the app to function properly.

For example, they may pretend to be calling from a legitimate service provider to persuade the user to enable the permissions. After this they

can remotely receive all communications sent to the victim's phone, including one-time codes used for 2FA.

Although multiple conditions must be fulfilled for the aforementioned attack to work, it still demonstrates the fragile nature of SMS-based 2FA methods.

More importantly, this attack doesn't need high-end technical capabilities. It simply requires insight into how these specific apps work and how to intelligently use them (along with social engineering) to target a victim.

The threat is even more real when the attacker is a trusted individual (e.g., a family member) with access to the victim's smartphone.

What's the alternative?

To remain protected online, you should check whether your initial line of defense is secure. First check your password to see if it's compromised. There are a number of security programs that will let you do this. And make sure you're using a well-crafted password.

We also recommend you limit the use of SMS as a 2FA method if you can. You can instead use app-based one-time codes, such as through Google Authenticator. In this case the code is generated within the Google Authenticator app on your device itself, rather than being sent to you.

However, this approach can also be compromised by hackers using some sophisticated malware. A better alternative would be to use dedicated hardware devices such as YubiKey.

These are small USB (or near-field communication-enabled) devices that

provide a streamlined way to enable 2FA across different services.

Such physical devices need to be plugged into or brought into close proximity of a login device as a part of 2FA, therefore mitigating the risks associated with visible one-time codes, such as codes sent by SMS.

It must be stressed an underlying condition to any 2FA alternative is the user themselves must have some level of active participation and responsibility.

At the same time, further work must be carried out by service providers, developers and researchers to develop more accessible and secure authentication methods.

Essentially, these methods need to go beyond 2FA and towards a multi-factor authentication environment, where multiple methods of authentication are simultaneously deployed and combined as needed.

Provided by The Conversation

Citation: How hackers can use message mirroring apps to see all your SMS texts and bypass 2FA security (2021, August 16) retrieved 30 April 2024 from https://techxplore.com/news/2021-08-hackers-message-mirroring-apps-sms.html