OfReg Paper 2018-002

The Risks of Text Messages for User Authentication

Version: 0-1

Date: 25th May 2018

Authors: Alee Fa'amoe, Deputy CEO & Executive Director ICT
Ian Callow, Manager Fixed and Wireless Services

Contents

1. Introduction 2
2. Executive Summary 3
3. Background 4
4. The Problem 5
5. OfReg Recommendation 8

1. Introduction

While entering your username and password into your bank's online system, sometimes an additional step is required of you to respond to a text message sent to your mobile phone with a special code.

"Oh, this must be extra secure!" you think. Unfortunately, you'd be wrong.

Cybercriminals have found and exploited a weakness in mobile phone systems around the world to gain access to bank accounts and to steal thousands of dollars from unsuspecting customers. Unfortunately, sometimes the banks themselves were equally unaware of this vulnerability.

But it's not just banks that are exposed to this weakness. Any service provider anywhere in the world who uses SMS text messages as part of the authentication process for their customers' online accounts could be susceptible to a vulnerability that comes, not from their own systems, but from the telecommunications networks.

2. Executive Summary

Online systems which use SMS text messages as part of the user authentication process are subject to several well-known vulnerabilities:

- Malware on mobile 'phones which captures SMS messages;
- SIM Swap where a criminal uses personal information to persuade a carrier to transfer mobile service to a new SIM;
- Fake cell sites; and
- Exploitation of weaknesses in the mobile network signalling systems.

Cayman Islands service providers across private and public sectors, including financial services providers, are encouraged to avoid using SMS text messages in any part of their user authentication process.

3. Background

Readers may undoubtedly have a growing list of online accounts for such services as email, banking, airline reservations, social media, and the list goes on.

Several layers of authentication can be used to help secure user access and prevent unauthorised access to those accounts:

- Single factor authentication (SFA), generally something a person knows e.g. username/password combination, response to a simple question (what is the name of your pet?) etc;
- Two factor authentication (2FA) adds a second layer and is, generally, something a person possesses (e.g. mobile 'phone, security token etc.); and
- Three factor authentication (3FA) could be inherence factors i.e. something a person is (e.g. biometric information which includes physical characteristics like a fingerprint, behavioural like keystroke cadence etc.)

Each layer of authentication adds to the security of the process even if they have inherent vulnerabilities e.g. the answers to common security questions like "What is your mother's maiden name" are easily discovered.

When using a mobile phone as part of the 2FA, banks, cloud service providers, email and application providers, and other entities will often use text messaging. A message with a special code or a 'one time password' is sent to your mobile phone.

Typically, the mobile phones receive the messages over a service called Short Message Service or SMS. This is an industry-standard messaging protocol used by wireless carriers around the world.

The problem is – SMS is not secure.

This paper seeks to inform users, banks, service providers, government entities, and any mobile users in the Cayman Islands about the risks associated with SMS and related technologies.

4. The Problem

The use of mobile handsets and SMS presents several vulnerabilities for the interception of such messages:

- Malware on mobile 'phones which captures SMS messages;
- SIM Swap where a criminal uses personal information to persuade a carrier to transfer mobile service to a new SIM;
- Fake cell sites; and
- Exploitation of weaknesses in the mobile network signalling systems.

Malware such as com.pch.monitor-smsspy or SMS.Agent.apa (also known as Ustanovka.apk) can end up on mobile handsets. The malware, amongst other activities, will capture SMS messages and send them to the person or organisation responsible for the malware.

With SIM Swap the targeted individual will lose all service if their carrier transfers their service to another SIM which is in the possession of the criminal. The criminal will then receive all traffic intended for the victim. More information can be found on the web regarding this type of fraud including this article from Digital Trends[1].

Fake cell sites can be set up using readily available hardware and software running on a laptop. The weakness of this threat is that the criminal has to be relatively close to their target.

Mobile networks use a special system to send control signals between network elements and between different mobile provider networks to set up and release voice calls, update location information and to send and receive text messages over SMS.

These control signals are typically sent using an industry-standard signalling system known as Signalling System 7.

Recently there has been some publicity regarding the security of Signalling System Number 7 (SS7) and the use of SMS messages as part of a 2FA solution.

The use of SS7 signalling by criminals was shown in Germany when hackers diverted SMS messages used for authenticating bank transactions and stole

[1] https://www.digitaltrends.com/mobile/sim-swap-fraud-explained/ [accessed 6th December 2017]

money from people's bank accounts. A report on this activity can be found on the pymts.com website[2].

It is difficult to gain access to the SS7 signalling network, but as the attack in Germany demonstrated, it is possible. For these attacks to work, the criminals also need the username and password for the on-line bank account. These can be obtained either via a data breach or a phishing attack.

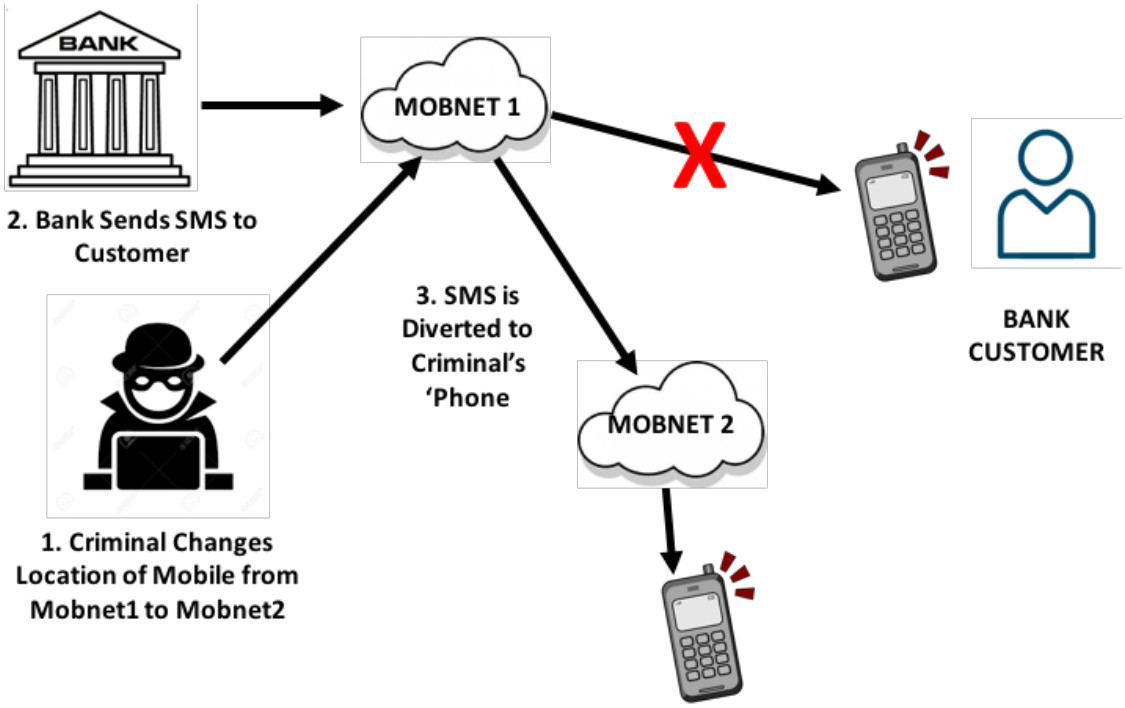

Diagram Illustrating the Diversion of SMS Messages

[2] https://www.pymnts.com/news/security-and-risk/2017/o2-confirms-hack-that-wiped-out-german-customer-bank-accounts-mobile/ [accessed 6th December 2017]

The National Institute of Standards and Technology (NIST) has recognised the risks of using SMS messages in authentication/authorisation systems. In the 800-63 series of documents[3], NIST has updated its Digital Identity Guidelines and provides guidance on the use of SMS as well as other methods of authentication.

There are steps that network operators can take that can reduce the risk of misuse of the SS7 system, however, the risk cannot be reduced to zero.

[3] https://pages.nist.gov/800-63-3/ [accessed 25th September 2017]

5. OfReg Recommendation

Unfortunately, there's no easy fix for this vulnerability. It's a global problem without a global solution at this point.

Even if every telecommunications provider in the Cayman Islands were to upgrade their systems, the fact is they will still have to connect to other telecommunications networks around the world using SS7 and similar systems. If those networks are not suitably protected, the vulnerabilities remain.

OfReg recommends therefore that Cayman Islands banks, government entities, service providers, utilities, insurance companies, and any other service provider with customers in the Cayman Islands, carefully review their processes for authorising digital transactions and avoid using SMS text messages in any part of the authentication process wherever possible.

---END---