James Moran
Head of Security,**GSMA**

GSMA Best Practice Recommendations

James Moran, Head of Security

Incentives to Counter SIM Swap

- Instances of SIM swap are increasing – driven by 2FA take-up
- SIM swap is a criminal offence and is being leveraged to commit crime
- Financial losses accruing to customers, banks and telcos
- Downstream impact of SIM swap is increasingly apparent
- Telco processes are being undermined and have local impact
- Reputational damage is being done to operators and their services
- Calls for liability to be examined are focussing minds
- Benefits of collaboration between telcos and financial services recognised
- Desire to protect all of our customers
- Technical means exist but focus also needed on processes

Fraud and Security Group (FASG)

Over
1400
Members

Fraud & Security management professionals

Collaborative industry action

5 Subgroups

DSG | FSAG | FSC
RIFS | SECAG

Information sharing alerts & education on risks trends defences

Focus areas

- Technical initiatives
- Roaming and interconnect
- Device security
- Security certification schemes

Fraud and Security Group Mission

Centre Of Expertise

Drive industry management of mobile fraud and security

Trusted Environment

Provide a trusted environment for discussing fraud and security matters.

Increase Protection

Mobile operator technology & infrastructure

Customer identity security and privacy

Reputation

Maintain industry reputation and trust in mobile operators and services

Fraud and Security Group Work Areas

Device Security (DSG)	Roaming & Interconnect (RIFS)	Security Architecture (FSAG)	Fraud & Security Comms (FSC)	Security Assurance (SECAG)
• *5G device identifiers* • *eUICC profile device blocking* • *DHS mobile security report analysis* • *Software updates for IoT devices*	• *SS7 vulnerabilities* • *Diameter & GTP security* • *Roaming fraud management (incl. CAMEL)*	• *False base station detection* • *UICC security guidelines* • *2G/3G switch off security guidelines* • *NFV security* • *CLI spoofing*	• *Best practice & intelligence sharing on fraud & security management* • *Education & awareness of new and evolving threats*	• *Infrastructure security & testing* • *Supplier security certification schemes (e.g. SAS, NESAS)*

GSMA Resources – One Page Brief

- Defines the issue
- Provides guidance on how to detect
  1. Monitor account changes
  2. Monitor customer complaints
  3. Monitor calls to customer service
  4. Send SMS confirmation to customers
- Outlines 10 defence mechanisms

ACCOUNT TAKEOVER

WHAT IS ACCOUNT TAKEOVER?

A fraudster hijacks an existing open account within the mobile operator. A fraudster performs an account takeover to obtain goods for re-sale, to artificially inflate traffic, or to perform banking fraud, or direct carrier billing fraud by compromising the SMS channel used for out of band two-factor authentication.

HOW TO DETECT SIM SWAP ATTACKS IN A MNO

1 Monitor account changes on CRM system
- Suspicious activity sequences and timelines
- Patterns of upgrade resetting
- Add-on activity
- SIM replacement activity

2 Monitor customer complaints
- Upgrades performed without customer authorisation
- Password/account change complaints
- Payments/charges complaints

3 Monitor calls into customer service
- Off network calls into customer service
- Calls into specific routes/teams
- Monitoring interactive voice response selections and pathways

4 Send SMS confirmations to customer
- After change of password; address; activation of additional service; product order
- As part of the mobile number porting (MNP) process (opt in)
- After request for SIM replacement/additional SIM

For more information, please see FF.21 Fraud Manual on InfoCentre², or contact us via gsma.com/security

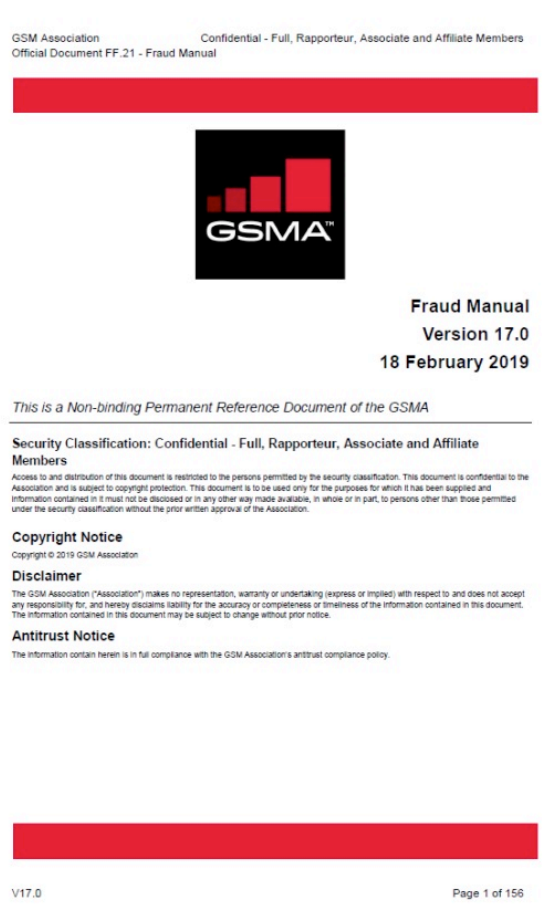
Fraud and Security Group

BEST DEFENCE MECHANISMS

- Equal level of customer validation for new and existing customers
- Create awareness of social engineering and account takeover risks and defences amongst customers
- Education and training of sales/dealer staff
- Geographical feasibility check to detect excessive distance between the SIM swap location and the location of the active SIM
- Implement firewalls (SS7, Diameter, SMS) on the network
- Consider implementing GSMA Mobile Connect in order to authenticate users
- Co-operate with banks and police to help prevent banking fraud
- Introduce strong controls on issuing of blank SIM cards
- Refer SIM replacements to a centralised team rather than handle at retail outlets, to ensure best practise is always followed
- Introduce validation processes and notifications on account changes/updates e.g. send confirmation SMS to the currently active SIM.

GSMA Resources – Fraud Manual

- Produced and maintained by FASG
- Reference guide to fraud for GSMA members
- Describes frauds that affect mobile networks
- Provides standard terms and definitions
- Covers 49 fraud types across 5 domains
  1. Technical Fraud
  2. Subscription Fraud
  3. Distribution Fraud
  4. Business Fraud
  5. Prepaid Fraud
- SIM Swap



GSM Association Confidential - Full, Rapporteur, Associate and Affiliate Members
Official Document FF.21 - Fraud Manual

GSMA

Fraud Manual
Version 17.0
18 February 2019

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Confidential - Full, Rapporteur, Associate and Affiliate Members

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2019 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

V17.0 Page 1 of 156

Princeton University Study – March 2020

- Examination of customer authentication processes at 5 carriers
- Found that all carriers use insecure authentication challenges
- Acknowledged trade-off between security and usability
- Noted different security levels between prepaid and post paid
- Highlighted impact on security policies using phone based authentication
- Ownership of the problem highlighted as being an issue

An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee Ben Kaiser Jonathan Mayer Arvind Narayanan
Department of Computer Science and Center for Information Technology Policy
Princeton University

Draft — March 25, 2020

Abstract

We examined the authentication procedures used by five prepaid wireless carriers when a customer attempted to change their SIM card. These procedures are an important line of defense against attackers who seek to hijack victims' phone numbers by posing as the victim and calling the carrier to request that service be transferred to a SIM card the attacker possesses. We found that all five carriers used insecure authentication challenges that could be easily subverted by attackers. We also found that attackers generally only needed to target the most vulnerable authentication challenges, because the rest could be bypassed. Authentication of SIM swap requests presents a classic usability-security trade-off, with carriers underemphasizing security. In an anecdotal evaluation of postpaid accounts at three carriers, presented in Appendix A, we also found—very tentatively—that some carriers may have implemented stronger authentication for postpaid accounts than for prepaid accounts.

To quantify the downstream effects of these vulnerabilities, we reverse-engineered the authentication policies of over 140 websites that offer phone-based authentication. We rated the level of vulnerability of users of each website to a SIM swap attack, and have released our findings as an annotated dataset on `issms2fasecure.com`. Notably, we found 17 websites on which user accounts can be compromised based on a SIM swap alone, i.e., without a password compromise. We encountered failures in vulnerability disclosure processes that resulted in these vulnerabilities remaining unfixed by nine of the 17 companies despite our responsible disclosure. Finally, we analyzed enterprise MFA solutions from three vendors, finding that two of them give users inadequate control over the security-usability tradeoff.

1 Introduction

Mobile devices serve many purposes: communication, productivity, entertainment, and much more. In recent years, they have also come to be used for personal identity verification, especially by online services. This method involves sending a single-use passcode to a user's phone via an SMS text message or phone call, then prompting the user to provide that passcode at the point of authentication. Phone-based passcodes are frequently used as one of the authentication factors in a multi-factor authentication (MFA) scheme and as an account recovery mechanism.

To hijack accounts that are protected by phone-based passcode authentication, attackers attempt to intercept these passcodes. This can be done in a number of ways, including surveilling the target's mobile device or stealing the passcode with a phishing attack, but the most widely reported method for intercepting phone-based authentication passcodes is a SIM swap attack. By making an unauthorized change to the victim's mobile carrier account, the attacker diverts service, including calls and messages, to a new SIM card and device that they control.

SIM swap attacks allow attackers to intercept calls and messages, impersonate victims, and perform denial-of-service (DoS) attacks. They have been widely used to hack into social media accounts, steal cryptocurrencies, and break into bank accounts [1–3]. This vulnerability is severe and widely known; since 2016 NIST has distinguished SMS-based authentication from other out-of-band authentication methods due to heightened security risks including "SIM change" [4].

SIM swap procedures have valid purposes: for example, if a user has misplaced their original device or acquired a new device that uses a different size SIM card slot than the device it is replacing. In these cases, customers contact their carrier (often by calling the carriers' customer service line) to request a SIM card update on their account. The customer is then typically presented with a series of challenges that are used to authenticate them. If the customer is successfully authenticated, the customer service representative (CSR) proceeds to update the SIM card on the account as requested.

We examined the types of authentication mechanisms in place for such requests at five U.S. prepaid carriers—AT&T, T-Mobile, Tracfone, US Mobile, and Verizon Wireless—by signing up for 50 prepaid accounts (10 with each carrier)

1

SIM Swap – Modus Operandi

- Goal is to (by-)pass validation checks and gain access to accounts
- Dependent on processes being targeted – requires knowledge and information
- Social engineering of customers to obtain personal and account information
- Social engineering of agents to obtain information/access and test processes
- Manipulation of lost and stolen reporting services with lower verification needs
- Internal or sales channel compromise to obtain customer details and target lists
- In store/retail channel attendance to execute transactions
- Caller line identity spoofing to bypass CLI access controls

SIM Swap – Proactive Detection Advice

1. **Monitor account changes** on CRM systems for suspicious activity sequences, upgrade patterns, add-on activity, SIM swap activity origins, etc.
2. **Monitor deliveries and logistics** by location, look for multiple deliveries at or near single locations, activity patterns etc.
3. **Monitor calls to customer service**, particularly off-net calls, calls to specific routes/teams, interactive voice response selections and pathways, etc.
4. **Monitor customer complaints** involving unrequested upgrades, password/account changes, payments/charges complaints
5. **Send SMS notification/confirmation** to customers following change of password, address, service activation, porting request, SIM replacement, etc.

SIM Swap – Best Prevention Advice

- Demand equal validation for new & existing customers
- Implement IP address controls on online channels
- Validate customer service calls by customer
- Introduce validation controls on device delivery
- Implement biometric voice recognition access control
- Implement biometric behaviour recognition access control
- Enforce time-based restrictions on account changes
- Implement firewalls (SS7, Diameter, SMS) on the network
- Implement SMS home routing
- Implement chargeable action controls on accounts
- Introduce validation & notification on changes/updates
- Educate and create awareness amongst customers
- Educate and train sales/dealer staff
- Introduce strong controls on issue of blank SIM cards
- Activate SIM cards only when SIM order/delivery is confirmed by customer
- Control SIM activation without history of SIM order/dispatch
- Implement special surveillance steps within MNP process
- Contact the customer in the case of suspicious activity indications
- Exert good inventory controls on blank SIMs
- Co-operate with other stakeholders to prevent fraud
- Use geographical feasibility checks
- Request confirmation of changes via USSD
- Enhance controls to targeted accounts
- Allow customers to set higher levels of security

GSMA Proposed Action

- Much done … there is more to do
- Review effectiveness of best practice recommendations
- Understand obstacles that may exist to their implementation
- Increase awareness of best practice recommendations
- Look at impact of emerging technologies such as eSIM
- Work collaboratively with financial services through GSMA initiatives