Lost in Translation: Text Message Spoofing via Email

Sumanth Rao, Ye Shu, Stefan Savage, Aaron Schulman, Geoffrey M. Voelker, Enze "Alex" Liu
UC San Diego *Carnegie Mellon University*

IEEE S&P

1. Summary

- Attackers can send spoofed text messages as arbitrary senders using only the ability to send **email**.
- The attack abuses legacy "email to text" gateways that still convert **SMTP** email into **SMS/MMS** messages on carrier networks.
- By combining gateway flaws with how messaging apps merge conversations across **iMessage, RCS, SMS, phone numbers, and email addresses**, spoofed messages can appear inside **existing threads**.

All issues disclosed in the paper have since been patched or mitigated by **AT&T, Verizon, T-Mobile, Google Fi**, **Apple**, and **Google Msgs.**

2. Email to Text Gateways

AT&T
@txt.att.net
@mms.att.net

T-Mobile
@tmomail.net

verizon
@vtext.com
@vzwpix.com

Google Fi Wireless
@msg.fi.google.com

3. Sender identity conversion

Capture SMS / MMS PDU on an **Android phone**

SMTP Email
```
Mail From: <>
From: john.doe@state.gov
Subject: Travel Advisories
Body: You have an alert.
```

→

SMS PDU
```
Body: john.doe@state.gov
(Travel Advisories) You have
an alert.
```

All gateways supported **SPF**, **DKIM**, and **DMARC**; yet SMTP to IMS conversion logic exposed spoofing attacks



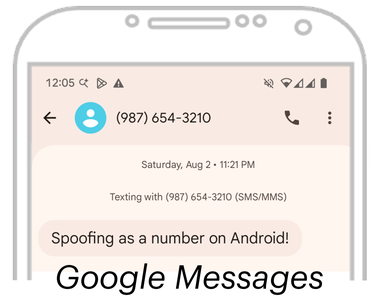
```
Mail From: <>
From: 987@6543.210
Body: Spoofing as a number on Android!
```

SMTP Email




```
Body: 987@6543.210
Spoofing as a number on
Android!
```

SMS



Google Messages

4. Spoofing via carrier gateways

Carrier Gateway	Basic	Mismatched Logic	Missing Header	Parsing Error
AT&T MMS	—	—	—	—
Google Fi MMS	MF: attacker.com F: example.com	MF: example.com F: attacker.com	—	—
Verizon SMS	MF: attacker.com F: example.com	—	MF: <> F: example.com	—
Verizon MMS	—	MF: example.com F: attacker.com	MF: <> F: example.com	—
T-Mobile SMS	MF: attacker.com F: example.com	—	MF: example.com	MF: attacker.com F: @user,@example.com:bad@attacker.com
T-Mobile MMS	MF: attacker.com F: example.com	—	MF: example.com	MF: attacker.com F: @user,@example.com:bad@attacker.com

Attacks exploiting vulnerabilities in carrier gateways (spoofing *example.com*)

5 .Spoofing as phone number

Apple iOS: iOS's Core Telephony layer **MIME-decodes** the sender field. The sequence **=?** (start of a MIME encoded-word) causes everything after it to be skipped.

→ Present in iOS binaries since at least iOS 9 **(2012)**

Android (Google Messages): Google Messages checks whether a sender is an email address using a regex that requires an **alphabetic TLD**. An all-**numeric address** like 987@6543.210 fails the check, so the app treats it as a phone number, strips @ and . and stores +1 (987) 654-3210.

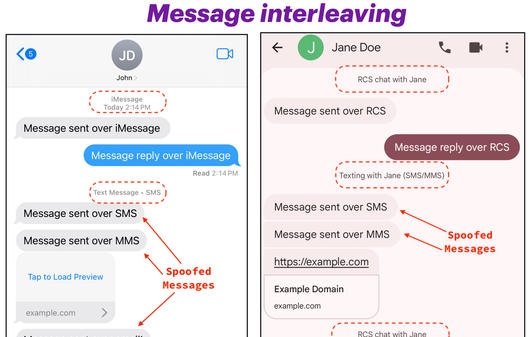
→ Present since at least Google Messages v2.0.068 (**2016**).

6. Parsing Vulnerabilities

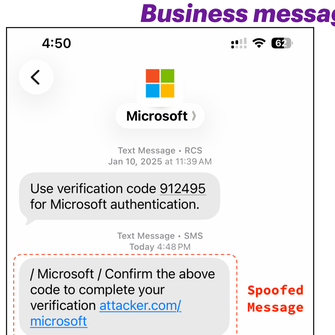
Parsing Vulnerability	Phone	Spoof As	Received As	Parsed As	Layer
Special Sequence	Apple	Phone Number Short Code Text	9876543210=?@attacker.com 54321=?@attacker.com Chase=?@attacker.com	+1 (987) 654-3210 54321 Chase	Telephony
Space	Apple	Phone Number Short Code Text	"9876543210 "@attacker.com "54321 "@attacker.com "Chase "@attacker.com	+1 (987) 654-3210 54321 "Chase	Telephony
Invalid Address	Apple	Phone Number Short Code Text	'9876543210' or "9876543210" '54321' or "54321" Chase	+1 (987) 654-3210 54321 Chase	Telephony
Numeric Address	Android	Phone Number Short Code	98766543.210 5@4.321	+1 (987) 654-3210 54321	Google Msgs

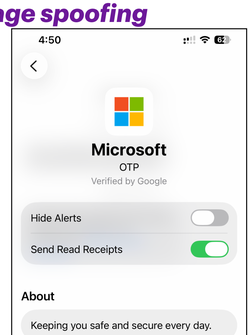
Parsing vulnerabilities in Apple and Android messaging stacks (attacker controls attacker.com)

Message interleaving

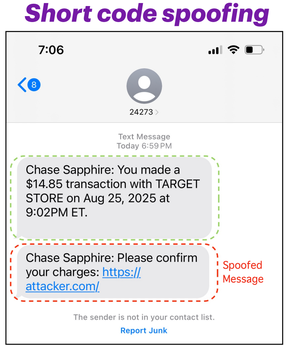


Business message spoofing





Short code spoofing



Group spoofing





Redirecting response

