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

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**.
- We evaluated the attacks across **AT&T, Verizon, T-Mobile, Google Fi,** and several smaller carriers on both iPhone and Android devices.
- All issues disclosed in the paper have since been patched or mitigated by **carriers**, **Apple**, and **Google**

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**

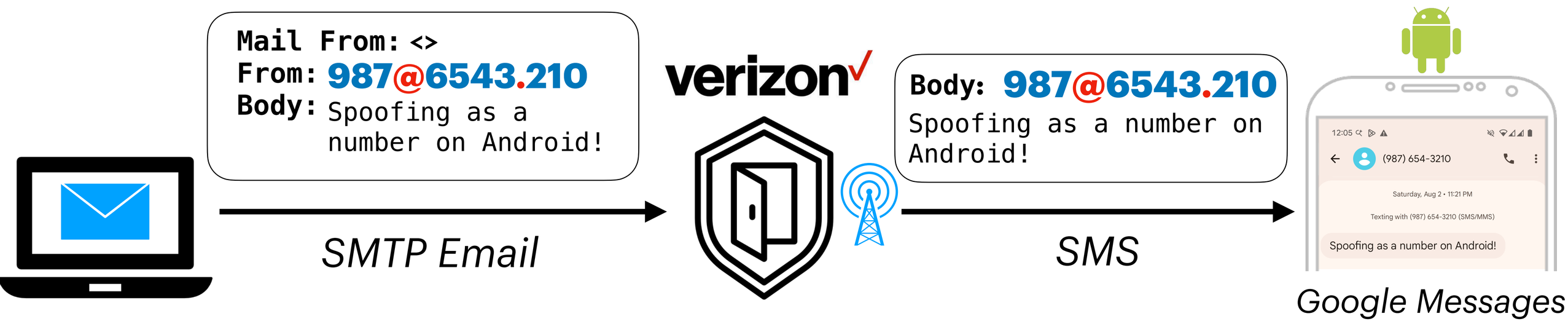
SMTP Email
```
Mail From: <>
From: john.doe@state.gov
Subject: Travel Advisories
Body: You have an alert.
```
→
SMS PDU
```
Body: john.doe@state.gov
(Travel Advisories) You have
an alert.
```

- All gateways supported **SPF**, **DKIM**, and **DMARC**; yet provider-specific conversion logic exposed spoofing attacks

4. Spoofing via carrier gateways

- Vulnerability of carrier gateways to various kinds of spoofing attacks (spoofing *example.com*)

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



5 .Spoofing as phone number

- **Apple iOS: "=?" truncation.** 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.
- We could (based on reverse engineering) ascertain that this bug has been in iOS binaries since at least **2012 (iOS 9)**
- **Android (Google Messages): numeric-email misparse.** 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**).

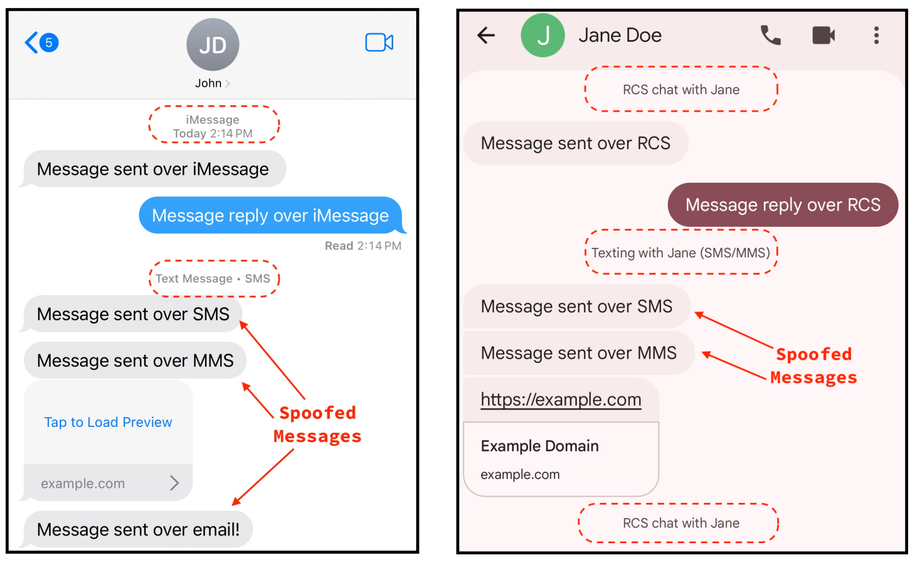
6. Parsing Vulnerabilities

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

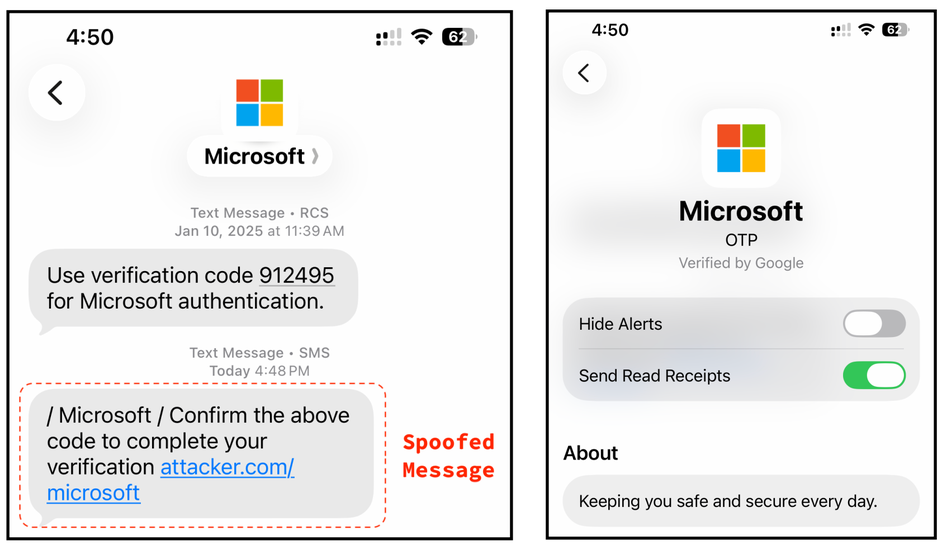
Parsing Vulnerability	Phone	Spoof As	Received As	Parsed As	Layer
Special Sequence	Apple	Phone Number Short Code Text	9876543210=?@attacker.com 54321=?@attacker.com Chase=?@attacker.com	+1 (987) 654-3210 54321 Chase	Telephony
Space	Apple	Phone Number Short Code Text	"9876543210 "@attacker.com "54321 "@attacker.com "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	987@6543.210 5@4.321	+1 (987) 654-3210 54321	Google Msgs

7. Capabilities

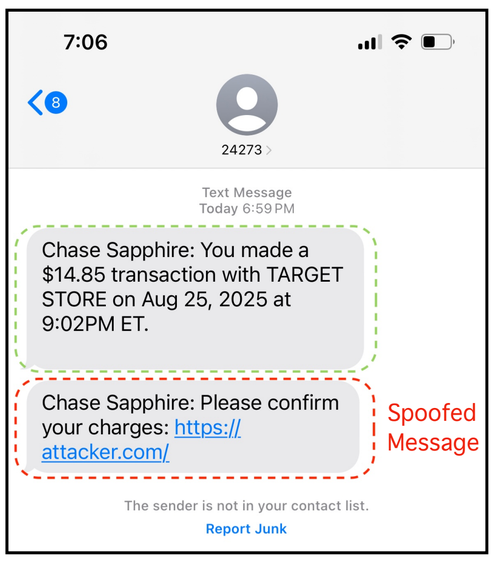
Message interleaving



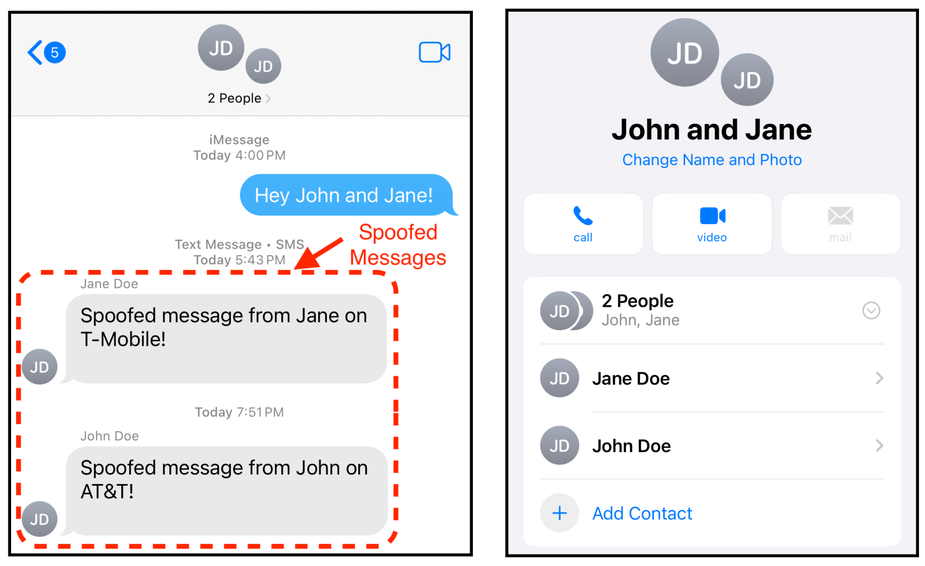
Business message spoofing



Short code spoofing



Group spoofing



Redirecting response