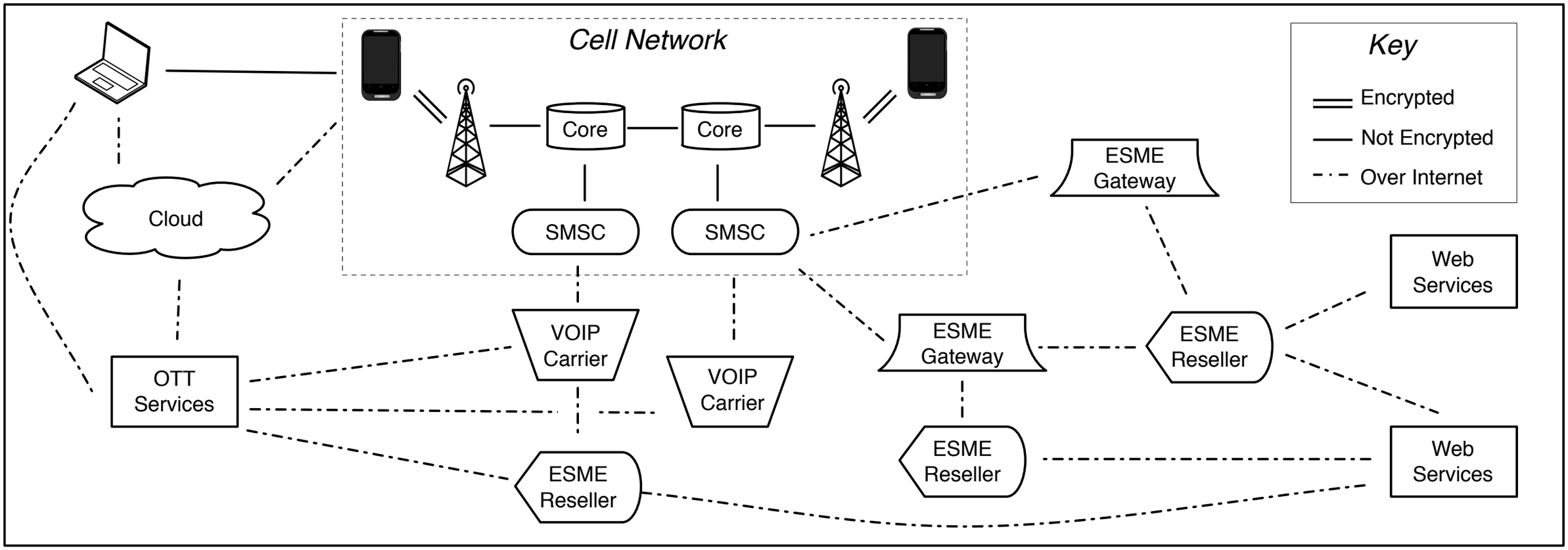
Sending out an SMS:

Characterizing the Security of the SMS Ecosystem with Public Gateways

Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, Kevin R. B. Butler

SMS Ecosystem

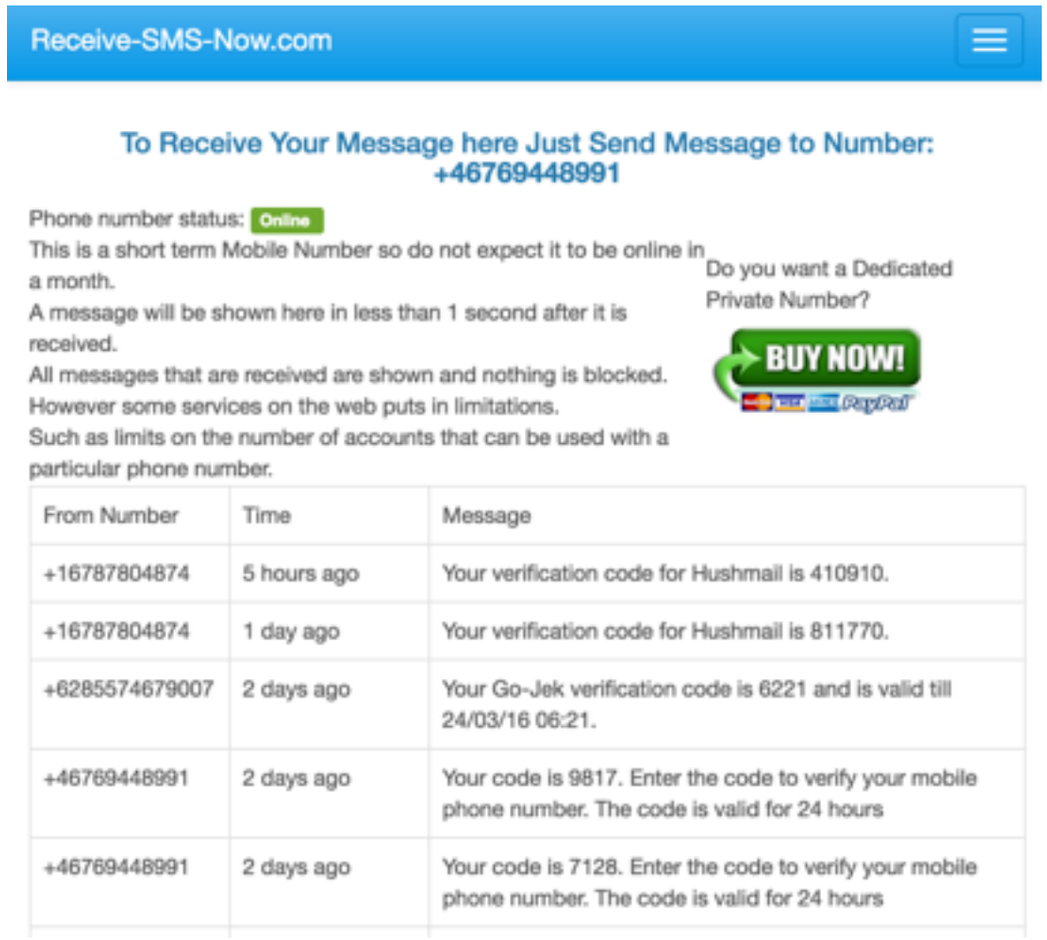


SMS is no longer a simple isolated channel
It has a broad attack surface

What is lost when a part of the ecosystem is compromised?

Public Gateway

- Data: 380k+ messages collected from 8 public gateways in 28 countries over 14 months
- These websites advertise themselves as a way to avoid spam or unwanted callers
- We'll divide our analyses into *uses* and *abuses*



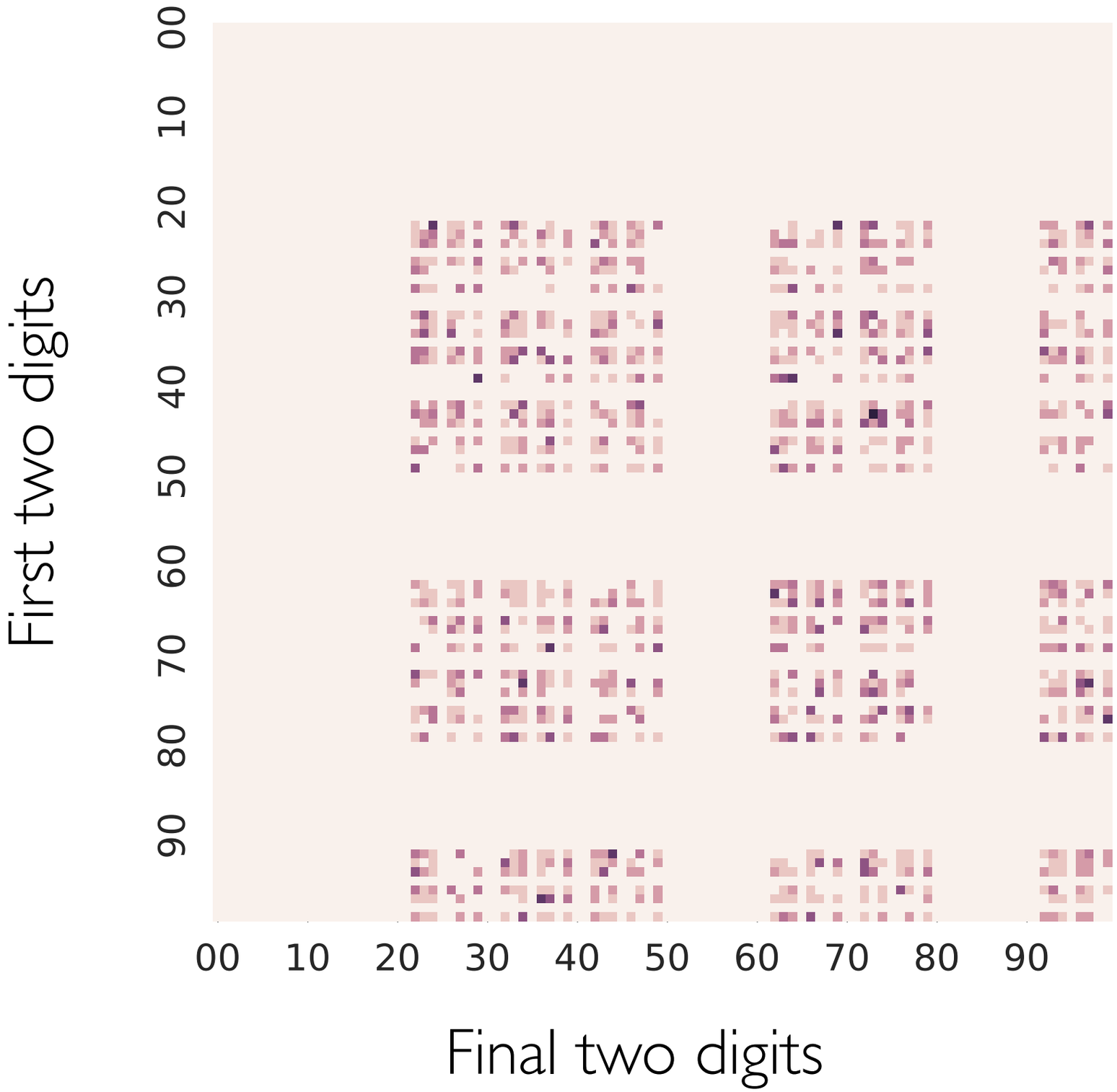
Ethics

The paper features an extensive ethics discussion

- The bulk of this data is sent to gateways by institutions, but the data also includes personal messages and PII
- This is already public data, and it is clear to users that this data will always be public

- **We cannot and do not attempt to deanonymize, track, identify, exploit, or otherwise use the personal information of any users and we systematically exclude personal messages**

OTP / Verification Codes



LINE

No Leading 0's

WeChat

rand()<<4 mod10000

Talk2

?

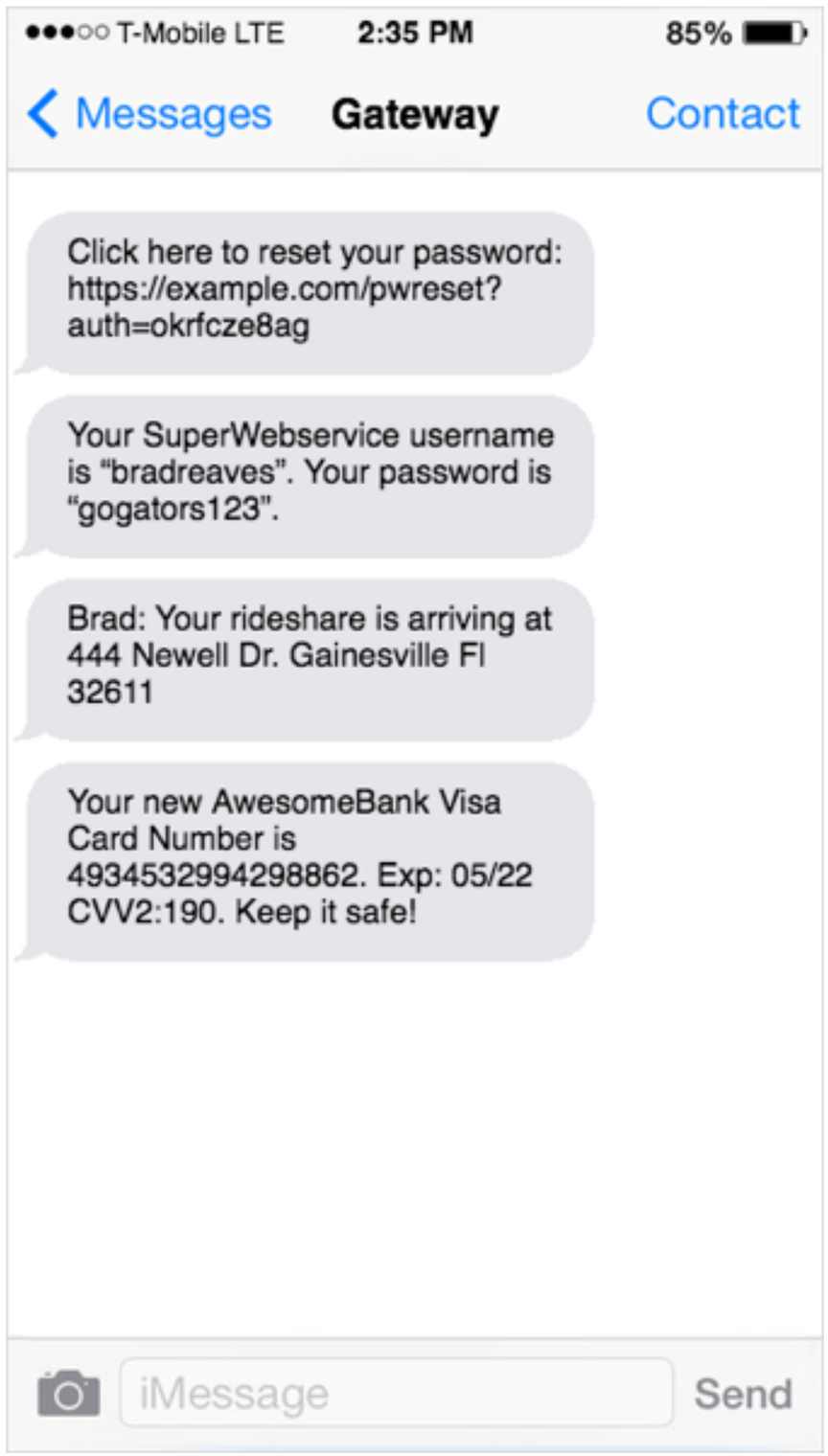
OTP / Verification Codes

Service	Uniform?	p-value	Effect Size (w)	Effect?	Mean Code
Google	✗	0.000	0.721	Large	547948
Google	✗	0.000	0.793	Large	558380
Instagram	✗	0.000	0.622	Large	503172
Instagram	✗	0.000	0.574	Large	498365
Instagram	✗	0.000	0.600	Large	497936
Jamba	✗	0.000	6.009	Large	4719
LINE	✗	0.000	0.595	Large	5476
LINE	✗	0.000	0.519	Large	5530
LINE	✗	0.000	0.530	Large	5442
Microsoft	✗	0.000	2.929	Large	357494
Odnoklassniki	✗	0.000	0.675	Large	433997
Origin	✗	0.000	0.512	Large	502627
QQ	✗	0.000	0.522	Large	505555
SMSGlobal	✗	0.000	0.500	Large	5540
Talk2	✗	0.000	1.327	Large	5732
Telegram	✗	0.000	0.478	Medium	54961
Viber	✗	0.000	8.138	Large	112075
WeChat	✗	0.000	0.664	Large	4989
Alibaba	✓	0.988			548652
Backslash	✓	0.325			556223
Baidu	✓	0.015			505165
BeeTalk	✓	0.595			544719
Circle	✓	0.080			506514
Gett	✓	0.461			5512
Google	✓	0.917			501623
Hushmail	✓	0.527			503161
LINE	✓	0.698			5511
Origin	✓	0.086			500739
RunAbove	✓	0.427			494697
Skout	✓	0.004			5492
Tuenti	✓	0.981			5010
Weibo	✓	0.395			512458
WhatsApp	✓	0.022			543563

χ-squared test for random distribution of PINs

13 Services fail to send a random code each message

Misuse: PII in SMS



Password Resets

Usernames and Passwords

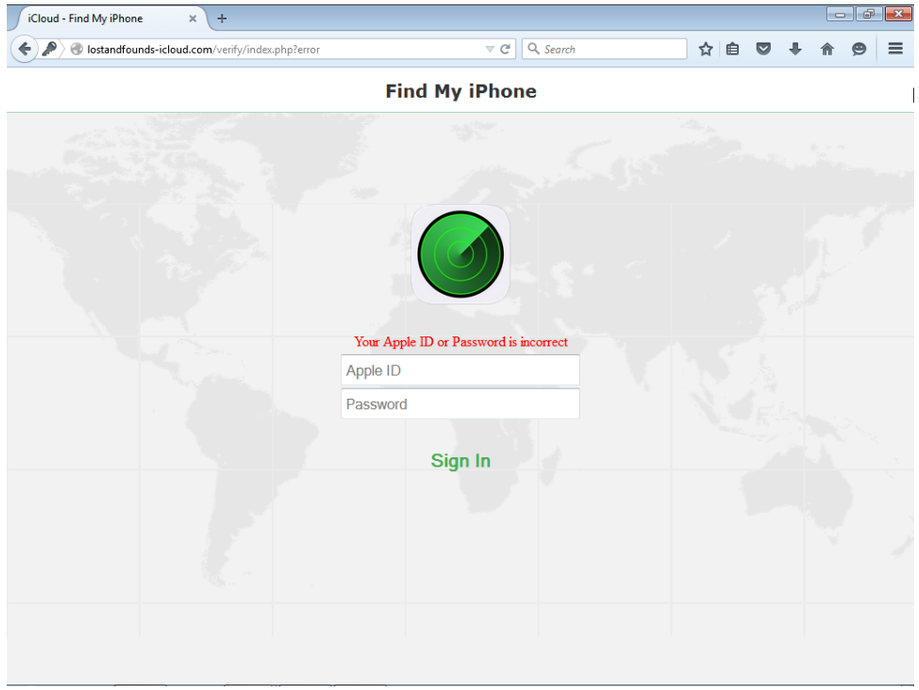
Names and Addresses

Credit Card Numbers

All sent over a channel *believed* to be secure

Abuse: Spam and Phishing

- ~1% of messages were spam
- We identified one long-running SMS phishing campaign
- *Malicious SMS activity is a real but relatively small phenomenon*

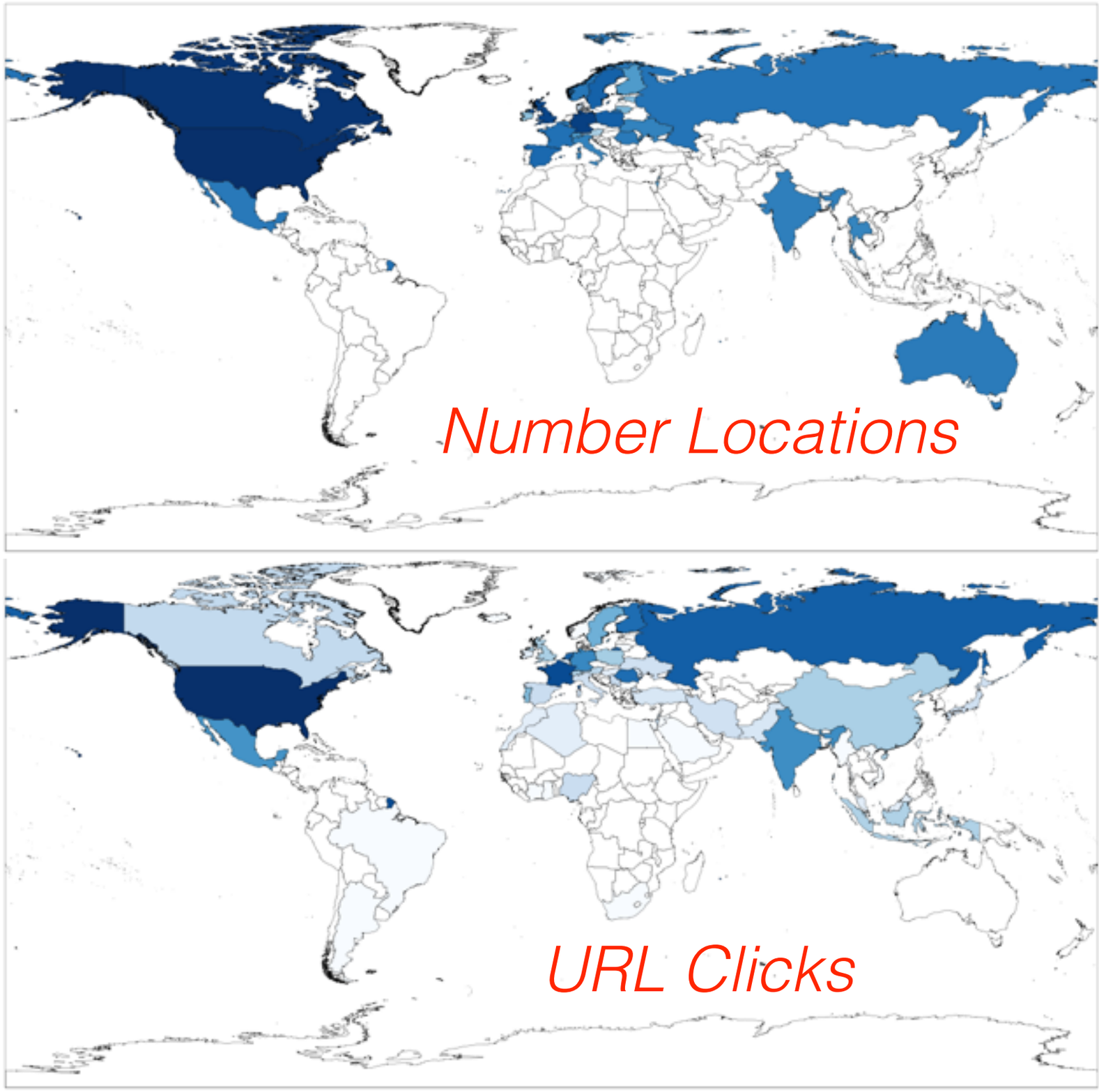


Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R. B. Butler "Detecting SMS spam in the age of legitimate bulk messaging" to appear at WiSec July 2016

Phone Verified Accounts

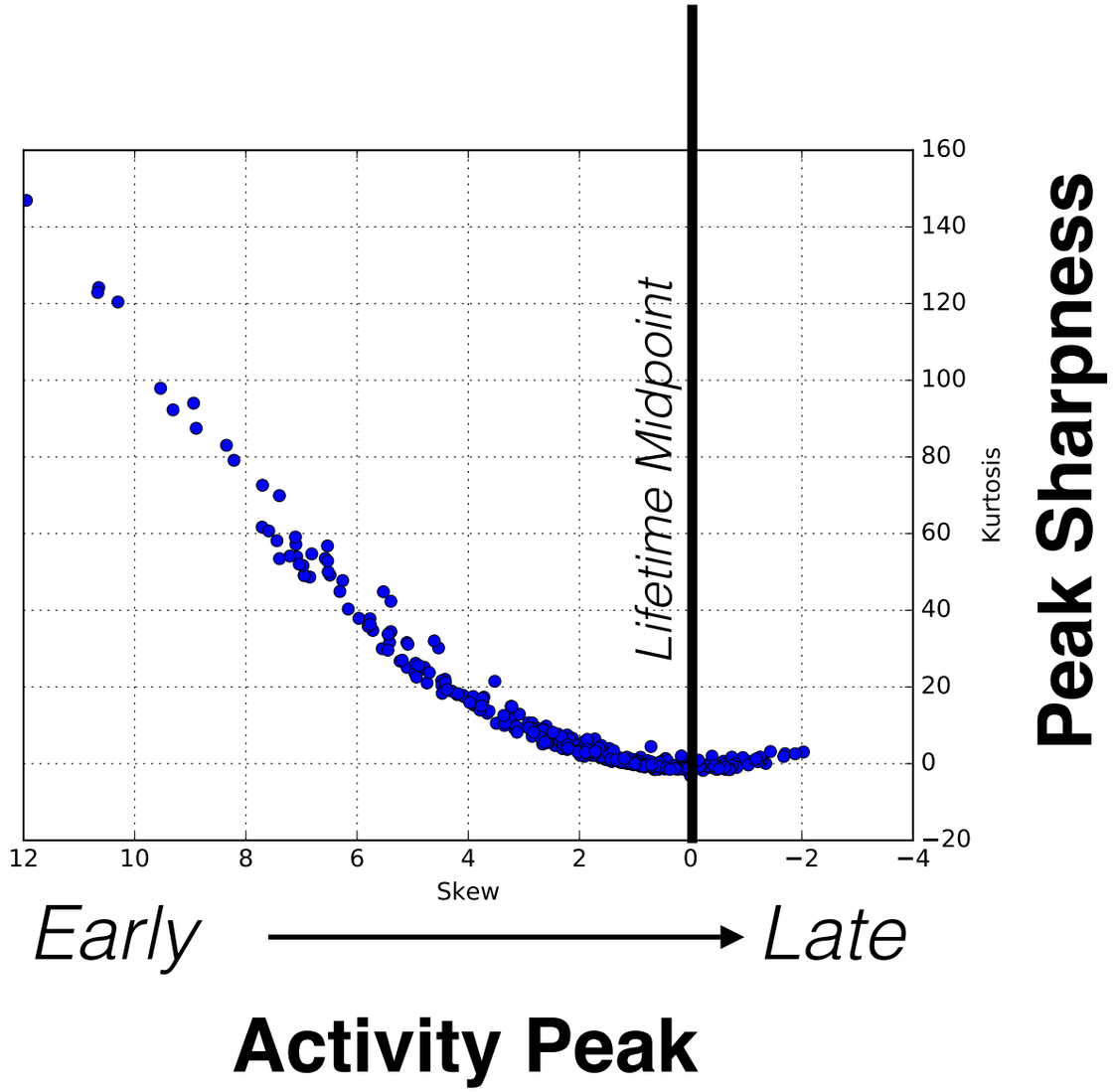
Abuse: Geo-Fencing

- Messages to *numbers in countries* are often viewed *outside of those countries*.
- Shortened URL services provide country-level statistics.



Abuse: Phone Verified Accounts

- Many of these gateways advertise as a means of evading PVA systems.
- Skew and kurtosis calculations show rapid use when numbers are introduced, followed by rapid decline.



Phone Verified Accounts

Thomas et al. (CCS '14) suggested 3 defenses:

1. Have users reverify often
   - Our numbers have a median life of *20 days*
2. Block numbers in low-reputation carriers
   - Most of our numbers are in reputable carriers
3. Block similar numbers
   - ~40% of numbers were similar, but only in mobile carriers

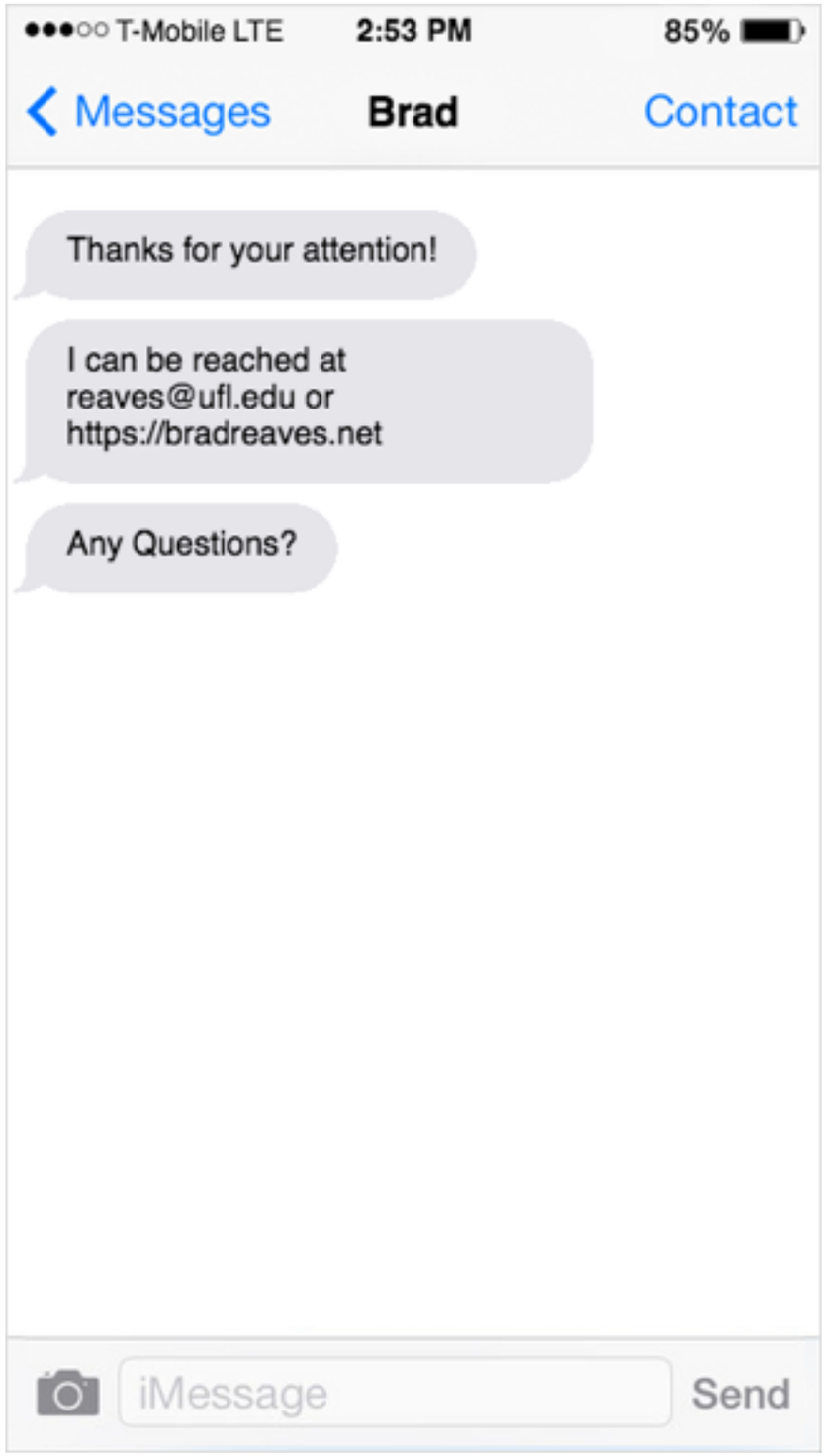
PVA Evasion is hard to detect or prevent

Takeaways

- Online gateways give us insight into how SMS is used and abused in the modern SMS ecosystem

- Organizations regularly use SMS as a secure channel for sensitive information despite risks of compromise

- Gateway data provides insights into spam, phishing, and phone verified account fraud


T-Mobile LTE
2:53 PM
85%
Messages
Brad
Contact
Thanks for your attention!
I can be reached at reaves@ufl.edu or https://bradreaves.net
Any Questions?
iMessage
Send