Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways

Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin R.B. Butler
Florida Institute for Cybersecurity Research (FICS)
University of Florida
{reaves, scaife, daveti, bluel}@ufl.edu, {traynor, butler}@cise.ufl.edu

***Abstract*—Text messages sent via the Short Message Service (SMS) have revolutionized interpersonal communication. Recent years have also seen this service become a critical component of the security infrastructure, assisting with tasks including identity verification and second-factor authentication. At the same time, this messaging infrastructure has become dramatically more open and connected to public networks than ever before. However, the implications of this openness, the security practices of benign services, and the malicious misuse of this ecosystem are not well understood. In this paper, we provide the first longitudinal study to answer these questions, analyzing nearly 400,000 text messages sent to public online SMS gateways over the course of 14 months. From this data, we are able to identify not only a range of services sending extremely sensitive plaintext data and implementing low entropy solutions for one-use codes, but also offer insights into the prevalence of SMS spam and behaviors indicating that public gateways are primarily used for evading account creation policies that require verified phone numbers. This latter finding has significant implications for research combatting phone-verified account fraud and demonstrates that such evasion will continue to be difficult to detect and prevent.**

I. Introduction

Text messaging has become an integral part of modern communications. First deployed in the late 1990s, the Short Messaging Service (SMS) now delivers upwards of 4.2 trillion messages around the world each year [70]. Because of its ubiquity and its perception as providing a secondary channel bound tightly to a user's identity, a range of organizations have implemented security infrastructure that take advantage of SMS in the form of one-time codes for two-factor authentication [10], [26], [36] and account validation [73].

The text messaging ecosystem has evolved dramatically since its inception, and now includes a much wider range of participants and channels by which messages are delivered to phones. Whereas phone numbers once indicated a specific mobile device as an endpoint and were costly to acquire, text messages may now pass through a range of different domains that never touch a cellular network before being delivered to a non-cellular endpoint. Moreover, these systems allow users to send and receive messages for free or low cost using numbers not necessarily tied to a mobile device, specific geographic area or even a single customer. As such, they violate many of the assumptions upon which the previously mentioned security services were founded.

In this paper, we perform the first longitudinal security study of the modern text messaging ecosystem. Because of the public nature of many SMS gateways (i.e., messages are simply posted to their websites), we are able to gain significant insight into how a broad range of companies are implementing SMS-based security services. Moreover, these systems allow us to see the ways in which defenses such as phone-verified accounts (PVAs) are successfully being circumvented in the wild. Our work makes the following contributions:

- **Largest Public Analysis of SMS Data:** While others have looked at aspects of SMS security in the past [37], [38], ours is the largest and longest study to date. Our analysis tracks over 400 phone numbers in 28 countries over the course of 14 months, resulting in a dataset of 386,327 messages. This dataset, which is orders of magnitude larger than any previous study of SMS, allows us to reason about the messaging ecosystem as a whole, which has not been possible in previous public studies.
- **Evaluation of Security Posture of Benign Services:** We observe how a range of popular services use SMS as part of their security architecture. While we find many services that attempt to operate in a secure fashion, we identify a surprising number of other services that send sensitive information in the clear (e.g., credit card numbers and passwords), include identifying information, and use low entropy numbers for their one-use codes. Because there is no guarantee that this channel is indeed separate, such observations create the potential for attacks.
- **Characterization of Malicious Behavior via SMS Gateways:** We cluster and characterize the lifetime, volume and content of the traffic seen in SMS gateways. Our analysis uncovers numerous malicious behaviors, including bulk spam and phishing. Most critically, our data shows that these systems are being used to support phone-verified account fraud, and the ways in which these systems are used makes proposed mitigations from previous work [72] largely ineffective.

We note the very fact that some users are willing to intentionally direct text messages to public portals is obviously dangerous. We do not address this phenomenon and instead focus on the risks of compromise of the SMS channel. Because these messages are known by the recipient to be publicly available, this dataset would naturally not be entirely representative of *all* SMS activity of a typical user. Nevertheless, this dataset enables the first public insights into issues such

DOI 10.1109/SP.2016.28

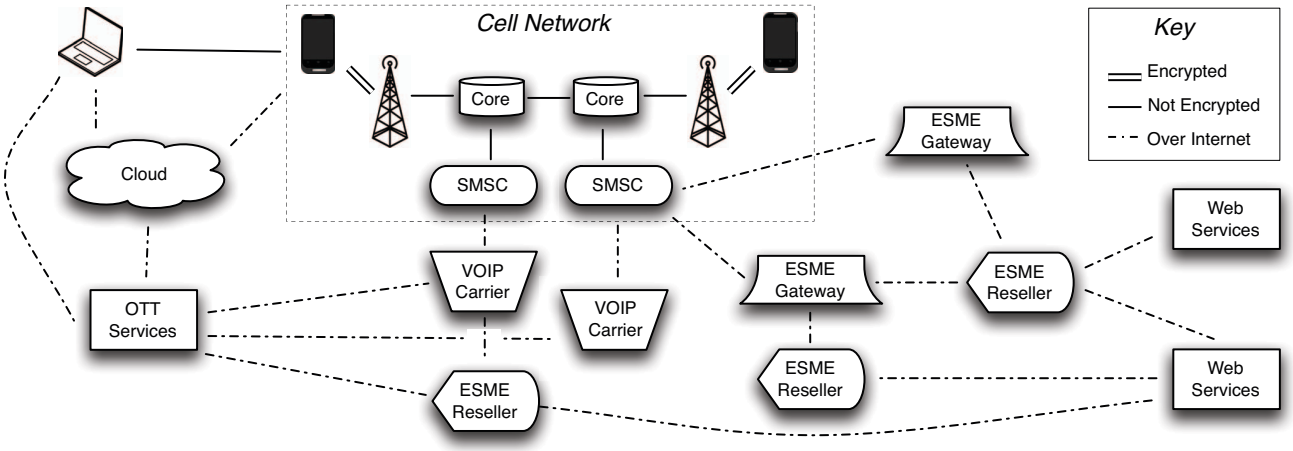


Fig. 1: While viewed as existing solely within cellular networks, the modern SMS ecosystem includes a wide variety of non-traditional carriers, ESME gateways and resellers, and OTT services. This evolution challenges old assumptions (e.g., phone numbers represent mobile devices tied to a single identity) and create new opportunities for interception. Accordingly, evaluating the state of this ecosystem is critical to understanding the security it provides.

as PVA scams, SMS spam, and sensitive information sent by legitimate services. Furthermore, this data is widely available to the community for continued evaluation and measurement in the future.

The remainder of the paper is organized as follows: Section II discusses the modern SMS ecosystem, which includes and extends beyond traditional cellular infrastructure; Section III discusses our collection and analysis methodology; Section IV characterizes our dataset; Section V discusses our analysis on legitimate usage of SMS via the gateways; Section VI discusses the malicious behaviors seen in our dataset. Section VII analyzes related work and Section VIII provides concluding remarks.

II. The Modern SMS Ecosystem

In this section, we describe at a high level how text messages are sent and received, with a special emphasis on recent developments that have greatly expanded the SMS ecosystem.

Figure 1 shows the components of the modern SMS ecosystem in detail. Short Messaging Service Centers (SMSCs) route messages through carrier networks and are the heart of the SMS system [79]. These entities receive inbound text messages and handle delivery of these messages to mobile users in the network using a store-and-forward regime similar to email. When a mobile device sends or receives a text message, the message is encrypted between the phone and the base station serving the phone; however, once inside the core network the message is typically not encrypted.

Text messages [1] are not just sent between individuals, but also by parties external to the network known as External Short Message Entities (ESMEs). ESMEs form an entire industry dedicated to facilitating the sending and receiving of messages for large-scale organizations for purposes as diverse as emergency alerts, donations to charities, or receiving one-time passwords [76]. These ESMEs act as gatekeepers and interfaces to SMS. Some have direct connections to SMSCs in carrier networks via SMPP (Short Message Peer-to-Peer) [66], while others resell such access purchased from other ESMEs. For example, the VoIP carrier Bandwidth.com provides SMS access to many third party services. Recently, startups like Twilio [22], Nexmo [11], and Plivo [15] serve as ESMEs and provide easy-to-deploy, low cost voice and SMS services. They serve a number of high-profile clients, including Uber, Coca Cola, and eBay.

Just as the methods for SMS distribution have evolved over the past two decades, how end users receive SMS has evolved as well. Originally, SMS were only delivered to mobile phones or to ESMEs. With the advent of smartphones, this ecosystem is changing rapidly. Over-the-top networks like Burner [3], Pinger [14], and Google Voice [6] provide SMS and voice services over data networks (including cellular data as well as Internet). Many of these services contract out to third party ESMEs for service and do not actually act as ESMEs themselves. Additionally, messages that are delivered to a mobile device may not remain restricted to that device. Systems like Apple Continuity [1], Google Voice, Pushbullet [16], and MightyText [9] use local wireless networks or cloud services to store and sync SMS from the receiving device to the user's other devices. Millions of subscribers use these services to transfer their messages from their localized mobile device to be stored in the cloud.

The modern SMS ecosystem has the consequence from a security perspective that a single SMS may be processed by many different entities — not just carriers — who *in toto* present a broad attack surface. Attacks against these systems may be technical in nature and take a form similar to publicized data breaches [52]–[54], [80]. While to date

[1] In this paper, we use SMS and "text message" interchangeably.

Site	Messages	Phone #s
(1) receivesmsonline.net	81313	38
(2) receive-sms-online.info	69389	59
(3) receive-sms-now.com	63797	48
(4) hs3x.com	55499	57
(5) receivesmsonline.com	44640	93
(6) receivefreesms.com	37485	93
(7) receive-sms-online.com	27094	19
(8) e-receivesms.com	7107	14

TABLE I: This table shows each of the SMS gateways we analyzed and the number of messages collected from each.

there are no disclosed attacks against these SMS services, we note that there is precedent for infiltration of carrier networks [81]. Social engineering attacks are also possible. Mobile Transaction Authentication Numbers (mTANs)[2] have been stolen using SIM Swap attacks [74] where an attacker impersonates the victim to a carrier to receive a SIM card for the victim's account, allowing the attacker to intercept security-sensitive messages. Attackers have also compromised accounts protected by one-time-passwords delivered over SMS by impersonating the victim to set up number forwarding to an attacker-controlled device [30]. Accordingly, it is worth determining what kinds of data are being sent via SMS so that the consequences of future compromise are well understood.

This work measures how different entities implement security mechanisms via text messages through the use of public SMS gateways. As such, we are able to observe a wide array of services and their behavior through time. Additionally, because these gateways provide phone numbers to anonymous users, we are also able to measure the extent to which such gateways are being used for malicious purposes. This combined measurement will help to provide the research community with a more accurate and informed picture of the security of this space.

III. Methodology

In this section, we describe the origins of our dataset, discuss some limitations of this dataset, discuss supplementary sources that give us additional insights into our SMS dataset, and finally describe the techniques we use to extract meaningful information from this dataset.

A. Public Gateways

In the previous section we noted that there are a number of organizations that process text messages, including carriers, ESMEs, resellers, and value-added services like message syncing. Within the category of ESMEs lie a niche class of operator: public SMS gateways. Many third party entities (including cellular carriers) provide external public interfaces to send text messages (but not receive them). Example use cases include the convenience of an email gateway or the ability to use a web service to send a message to a friend after one's mobile phone battery dies.

[2]mTANs are used to authenticate mobile banking transactions via SMS in many countries, including Germany, South Africa, and Russia.

While there are many public services for sending messages, they also have counterparts in public websites that allow anyone to *receive* a text message online. These systems publish telephone numbers that can receive text messages, and when a text message arrives at that number the web site publicly publishes the text message. These services are completely open — they require no registration or login, and it is clear to all users that any message sent to the gateway is publicly available. We recognized the research value of these messages for the potential to inform a data-driven analysis, and collected them over a 14 month period from 8 distinct public gateways that facilitate the receiving of text messages[3], listed in Table I. These gateways have similar names that are potentially confusing, so where appropriate we reference them by an assigned number 1—8 based on message volume. Despite their similar names, most of these services appear to be unaffiliated, and each has distinct hosting infrastructure. Gateways 4, 5, and 7 share 21 phone numbers, indicating a likely relationship between these gateways.

These different services have essentially the same functionality, but advertise their intended use in different ways. For example, Gateway 2 claims to be "useful if you want to protect your privacy by keeping your real phone number away from spammers," while Gateway 4 instructs users to "Enter the number where you want verify [sic] like Gmail, Yahoo, Microsoft, Facebook, Amazon, VK etc." Gateway 7 has perhaps the most specific use case: "When your ex-wife wants to send you a text message." Gateway 4 indicates that they expect users to use their service for account verification, while Gateways 2 and 7 simply advertise themselves as privacy services. We suspect that the business model of most of these websites relies on advertising revenue, and this is confirmed by at least Gateway 2, which prominently displays "almost all of [our income] comes from our online advertising" in a banner requesting that users disable their ad blocker. However, advertising is not the sole source of revenue for every system: Gateways 3, 4, 5, 6, and 8 sell private numbers for receiving SMS, while Gateways 4 and 5 actually sell verified Google Voice and WhatsApp accounts.

a) Ethical Considerations: As researchers, our ultimate goal is to improve the security practices of users and organizations, but we must do so ethically. In particular, we should make every effort to respect the users whose data we use in our studies.

A superficial ethical analysis would conclude that because it is clear that all messages sent to these gateways are public, and their use is strictly "opt-in", users have no reasonable expectation of privacy in the collection and analysis of this data. While we believe this analysis to be true, the situation is more complex and requires further discussion, as there are a number of parties to these messages. In addition to users who knowingly provide a gateway number as their own phone number, other individuals and institutions (companies, chari-

[3]Note that throughout the rest of the paper we use the term "gateway" to refer exclusively to these receive-only SMS gateways.

ties, etc.) may send information to individuals, not knowing that the messages are delivered to a public gateway. While institutions rightfully have privacy rights and concerns, they differ from those of individuals. As we show in our results, the vast majority of the information that we collect is sent indiscriminately and automatically by organizations to a large number of recipients. This information is unlikely to contain information that would negatively impact the institution if disclosed. Although we study bulk institutional messages, we do not analyze further those messages determined to be of a strictly personal nature. While those messages may have a research value, we *deliberately avoid these messages to prevent further propagating this data*.

Nevertheless, the use of gateways absolutely creates confidentiality and privacy concerns. For example, when personally identifying information (PII) or account credentials are sent to a gateway (whether or not all parties are aware), the compromise of that information is immediate and irrevocable [4]. Because we do not make our data available to others, this study does not change — in severity or duration — the harm done by the existence and use of the gateway. Furthermore, while in Section V-A we describe a host of sensitive information found in the dataset, we do not publish, use, or otherwise take advantage of this information. In particular, we especially do not attempt to access accounts owned by gateway users or operators.

We recognize that there are ethical questions raised not just with the collection of this data, but also by combining it with other data sources. Our data augmentation is sufficiently course-grained that no individual user of a gateway could be identified through our additional data [5]. Geographic information not already disclosed in text messages was limited to country-scale records in the case of gateway users and city-scale in the case of gateway numbers (which in any case do not likely correlate with the location of the gateway operator).

Overall, our hope is this study would raise awareness of the risks of sending sensitive information over insecure media and prevent future harm.

b) Limitations: To the best of our knowledge, this paper presents an analysis of the largest dataset of SMS published to date. However, there are some limitations to this data. First, because the messages are public, many services that use SMS (like mobile banking) are likely underrepresented in our dataset. For this reason, it is likely that our findings about sensitive data appearing in SMS are likely *underestimated*. Second, because gateways change their phone numbers with regularity, it is unlikely that long-term accounts can be successfully created and maintained using these numbers, which may bias the number of services we observe in our dataset. Accordingly, those users are unlikely to enable additional security services like mobile two-factor authentication (2FA) using one-time passwords (OTP), further limiting our visibility to a wider range of services. *These limitations mean that the overall distributions that we report may not generalize to broader populations.* Nevertheless, we believe that this work provides useful conclusions for the security community.

[4]Except perhaps by the gateway itself; however, it is clear from our data that gateways are not taking steps to prevent PII exposure

[5]The one exception to this was an individual whose information was used (likely without his/her knowledge) to register a domain used in a phishing scam. This information was discovered after a routine WHOIS lookup after discovering the phishing domain.

B. Crawling Public Gateways

To gather messages from gateways, we developed a web crawler using the Scrapy [19] framework. Every 15 minutes, our crawler connected to each gateway, obtained new messages, and stored these in a database. We faced two challenges to accurately recording messages: ignoring previously crawled messages and recovering message received times.

Ignoring previously crawled messages was difficult because gateways display the same messages for a considerable amount of time (days, months, or even years). A consequence of this is that our dataset contains messages that gateways received before our data collection began. In order to prevent storing the same messages repeatedly (and thus skewing the results), we discard previously crawled messages upon arrival by comparing the hash of a concatenation of the sender and receiver MSISDNs and the message content against hashes already in the database. If a match is found, the message sent times are compared to ensure that they were the same instance of that message, ensuring that messages that were repeatedly sent are still included in the data.

Message times required finesse to manage because gateways report a relative time since the message was received (e.g., “3 hours ago”) instead of an ideal ISO-8601 timestamp [69]. Parsing these timestamps is fairly simple, but care must be taken when doing comparisons using these times as the precision can vary (“3 minutes” vs. “3 days”). To ensure accuracy, we store and take into account the precision of every timestamp when comparing message timestamps.

C. Additional Data Sources and Analyses

1) Phone Number Analysis: After the scrapers pull the initial data from the gateways, the data is augmented with data from two outside sources. The first service, Twilio [22], provides a RESTful service that provides mobile, VoIP, and landline number look ups. Twilio resolves the number’s country of origin, national number format for that country, and the number’s carrier. Carrier information includes the carrier’s name, the number’s type, and the mobile network and country codes. Twilio is accurate and appropriately handles issues like number porting, which could cause inconsistencies in our data if incorrect.

The second service, OpenCNAM [12], provides caller identity information for North American numbers. This database contains a mapping of phone numbers and strings; carriers consult this database to provide Caller ID information when connecting a call. Therefore, OpenCNAM is also the most accurate public location to obtain identity information for North American numbers.

We obtained data from both Twilio and OpenCNAM for all the numbers that were hosted on the gateways as well as a subset of the numbers that contacted the hosted numbers.

2) URL Analysis: We extracted 20,793 URLs from messages by matching URL regular expressions with each message in the dataset. Overall, there were 848 unique second-level domains and 1,055 unique base URLs (fully-qualified domain names and IP addresses) in this set. For each of these domains, we obtained domain registration data. A domain's WHOIS registration data contains useful metadata about the history of a domain, including its creation date. Since this data is distributed among registrars, it is not always available and some fields may be restricted. We were able to obtain complete registration data for 532 of the second-level domains in our set.

Due to the limited length of an SMS message, shortened URLs are often sent in these messages. The short URL is a hop between the user and the destination, allowing URL shortening services to collect data about the users following the links. For each Bitly- and Google-shortened URL, we obtained statistics (e.g., number of clicks) when possible. The SMS gateway services do not publish data on their users, so this data represents one of the best insights into user demographics in our dataset.

Finally, since these gateways freely accept and publicly post SMS messages, the gateways represent an easy mechanism for delivering malicious messages including phishing or malicious URLs. VirusTotal [82] can provide valuable insight into the maliciousness of a given URL. We requested scans of each of the URLs via VirusTotal and collected the scan reports. If a URL had a previously-requested scan, we collected the cached scan and did not rescan the URL. Due to the short lifetimes of some malicious domains, we anticipated earlier scan results would be more accurate. For each product that VirusTotal uses to scan the URL, it reports whether or not the product alerted and if so, the category of detection.

3) Personally-Identifying Information Analysis: We searched the messages for personally-identifying information (PII) [58] using regular expressions. In particular, we searched for major credit card account numbers (e.g., Visa, Mastercard, American Express, Discover, JCB, and Diners Club). For each match, we further verified these numbers using the Luhn algorithm [57]. This algorithm performs a checksum and can detect small input errors in an account number. This checksum is built into all major credit card account numbers and can also assist in distinguishing a 16-digit Visa account number from a 16-digit purchase order number, for example. This check is rudimentary, however, and we manually verified the remaining matches to verify that they contextually appeared to be account numbers (i.e., the messages containing these numbers appeared to reference an account number).

Furthermore, we also checked strings of numbers to determine if they were identification numbers such as US Social Security Numbers or national identifiers from Austria, Bulgaria, Canada, China, Croatia, Denmark, Finland, India, Italy, Norway, Romania, South Korea, Sweden, Taiwan, or the United Kingdom. We found no valid matches in our data.

D. Message Clustering

A major goal of this study is to determine what types of messages are sent via SMS and how service providers are using SMS. While there are available machine learning techniques for this type of analysis and clustering (e.g., topic discovery and text clustering), scalability is a major problem when dealing with the large number of messages in our dataset. Accordingly, we explore other methods as described below.

Keyword Analysis. As a first attempt, we automatically labeled messages in the dataset using searches in multiple languages for keywords such as "password," "email," and "verification." We found that these keywords are often overloaded and insufficient for successfully separating the data. For example, Talk2 [21] uses "verification code" for the purpose of new account creation, while SMSGlobal [20] uses "verification code" for one-time passwords. Adding further complication, LiqPay [8] uses "password" for one-time passwords.

Furthermore, we identified messages that referenced our keywords without containing any obvious authentication data. These messages are often informative messages *about* the keywords (e.g., "Do not disclose your password."). Conversely, some messages containing sensitive information did not include keywords. Ultimately, the outcome of this experiment was unsuccessful, leading us to adopt a manual labeling approach.

Clustering Analysis. Through further analysis, we discovered that many messages from the same service provider share the same pattern. We manually reviewed messages and grouped similar messages together into "clusters"[6].

The essence of our clustering algorithm is distance-based clustering [42]. However, we wanted a high-accuracy clustering algorithm with minimal and easily estimated tuning parameters, ruling out k-means. We attempted to use an edit-distance metric to group similar messages into a connected graph (where edges are created between similar messages), but a pairwise algorithm exceeded the time and hardware available to the project. Instead, we noted that the messages we were interested in were virtually identical, apart from known common variable strings like `codes` or email addresses. By replacing these with fixed values, a simple lexical sort would group common messages together. We then identified cluster boundaries by finding where the normalized edit distance was lower than a threshold (0.9) between two consecutive sorted messages. Our threshold was was empirically selected to conservatively yield correct clusters, and we were able to cluster all 386,327 messages in a few minutes with high accuracy.

A more explicit statement of this process follows:

1) *Load all messages.*
2) *Preprocess messages by replacing numbers, emails and URLs with fixed strings.*

[6]Our definition of this term should not be confused with the classic machine learning definition of "clustering."

3) *Alphabetically sort preprocessed messages.*
4) *Separate messages into clusters by using an edit distance threshold to find dissimilar consecutive messages.*
5) *Manually inspect each cluster to label service providers, message types, etc. In this step, we culled clusters that had* < 43 *messages*[7].

Preprocessing is perhaps the most important step, because it allows us to avoid aligning messages from different service providers together. When using naive sorting on the original messages, the sorting places together messages from various services that start with a verification code. We avoid this problem by replacing variable content with a fixed string, causing the final sort order to be related to the non-variable content of the messages. Unlike traditional machine learning methods, our sorting-based clustering method is fast (minutes for our dataset).

After clustering, we *manually* labeled each cluster, a time-consuming process which allowed us to both verify the correctness of the cluster generation, and guarantees correct labels.

It is difficult to determine the intent of the message when the message contains little context (e.g. "X is your Google verification code."). For the most common 100 services, we attempted to identify message intentions using those services' public documentation. Where this information was unavailable, we attempted to register accounts with the services to obtain messages and match these to our clusters. If we were still unable to determine the message type, we classified these with a generic label. We also define and apply labels based on the overall content of the message, including content such as PII or any sensitive, security-related information.

E. Message Intentions

Due to the lack of standardized terms for the intentions of the authentication and verification values sent via SMS, we divided the various message *intentions* into categories in this section. In this paper, we use `code` to describe the value extracted from any message sent to a user for any of the below intentions. To our knowledge, there is no authoritative source for these intentions, despite their popularity. More than 261,000 (67.6%) of the messages contain a `code`, and the following categories enabled us to more accurately cluster our messages:

- **Account Creation Verification**: The message provides a `code` to a user from a service provider that requires a SMS verification during a new account creation.
- **Activity Confirmation**: The message provides a `code` to a user from a service provider asking for authorization for an activity (e.g., payment confirmation).
- **One-Time Password**: The message contains a `code` for a user login.
- **One-Time Password for Binding Different Devices**: The message is sent to a user to bind an existing account with a new phone number or to enable the corresponding mobile application.
- **Password Reset**: The message contains a `code` for account password reset.
- **Generic**: We use this category for any `codes` to which we are unable to assign a more specific intent.

[7]We initially planned on labeling only clusters with more than 50 messages, but our labelling process resulted in more labeled clusters than expected.

Country	Message Count	Number Count
United States	95138	98
Canada	77036	55
Germany	53497	46
United Kingdom	44039	75
Poland	16103	15
Sweden	14849	22
Spain	11323	11
France	8273	10
Russian Federation	7344	-
Norway	6674	8
Mexico	6431	5
Romania	6043	6
Australia	5964	13
Belgium	5253	3
India	5064	2
Ukraine	4363	3
Italy	4326	3
Thailand	4073	5
Hong Kong	3251	7
Israel	1971	5
Switzerland	1722	3
Finland	1714	13
Lithuania	520	1
Estonia	405	1
Ireland	331	3
Austria	158	2
Denmark	54	1
Czech Republic	6	2
Belgium	-	3

TABLE II: This table of gateway messages and numbers by country shows that gateways have an international presence, with most message volume taking place in North America and Western Europe. The message count represents the number of messages sent to numbers in each country.

IV. Data Characterization

In this section, we provide high-level information about our collected data. The dataset includes data from 8 gateways over 14 months. Overall, our dataset includes 386,327 messages sent from 421 phone numbers from 52 known carriers in 28 countries. Table II shows the message count for gateway phone numbers alongside the total number of gateway numbers by country.

1) Gateways and Messages: Table I shows the eight gateways we scraped, the number of messages from each, and the number of unique phone numbers hosted at each service during the collection time. The number of messages received by each gateway ranged from 7,107 to 69,389. The number of hosted numbers per service ranged from 14 to 93.

2) Infrastructure: We obtained detailed data from Twilio about the phone numbers in our dataset, as shown in Table III. Twilio identified 52 carriers, of which 46 are mobile, 3 are VoIP, and three are labeled as landline carriers. We believe that the numbers seen from these "landline" carriers are simply

Carrier Type	Amount	Percent of Total
Mobile	261	62.0%
VoIP	149	35.4%
Landline	11	2.6%

TABLE III: Using Twilio-provided data, we obtained the carrier type for each of the carriers associated with sender and receiver numbers on the gateways.

mislabeled as landlines by Twilio and are actually mobile numbers, due to all three being carriers that advertise both mobile and landline service. Furthermore, Twilio indicates numbers from `bandwidth.com` as "mobile" numbers (this is not due to porting, as Twilio resolves porting scenarios). `bandwidth.com` is actually a VoIP provider. The numbers in this paper are corrected to reflect this.

3) Geography: Twilio's number data also includes geolocation information for each number which shows our data is based in 28 countries. The United States has the most gateway controlled numbers with 98 numbers seen receiving 95,138 messages, the most traffic of any country. Conversely, Lithuania only had one gateway-controlled number registered to it, the lowest of the countries in our data. The Czech Republic has the fewest messages sent to the gateway-controlled numbers registered to a country, with two numbers receiving only six messages. Interestingly, 9 of our numbers are associated with providers who service the Channel Islands, located off the coast of France with a total population of less than 170,000 people.

Twilio data provides only the country of origin, so for all 153 numbers in the United States and Canada we obtain caller ID name (CNAM) data[8]. We found that the vast majority of numbers (55.4%) have no CNAM data at all. Of those messages that have data, the official record in the CNAM database is simply "CONFIDENTIAL," "WIRELESS CALLER," or "Unavailable." Note that "Unavailable" is the actual string that would be displayed to a user, not an indication of no data in the database.

The remainder of the messages are sent to phone numbers that have CNAM data indicating the number is in one of 57 cities or 3 provinces (British Columbia, Ontario, and Quebec) in the United States or Canada. By message volume, the top locations are "Ontario", followed by Centennial, CO (in the Denver area); San Francisco, CA; Little Rock, AR; Airdrie, AB; Columbia, SC; San Antonio, TX; Detroit, MI; Cleveland, OH; and Washington, MD. There are several observations to make from these findings: first, numbers are selected to well beyond what is likely the gateways' main location. Second is that neither gateways nor users feel a need to use numbers based in large population centers. With the exception of Centennial, CO, all locations had four or fewer numbers, regardless of population of the location. Gateways 4 and 5 registered the numbers in Centennial.

4) Clusters: We generated 44,579 clusters from our dataset. All messages with more than 43 messages were manually tagged and analyzed giving us 754 tagged clusters. These clusters represent the messages from the most popular services in our dataset. The tagged clusters only represent 1.7% of the total clusters but the tagged clusters cover 286,963 messages (74.2%). Figure 2 represents the data that supports this assertion by showing the exponential distribution of the cluster sizes.

[8]CNAM data only covers the US and Canada.

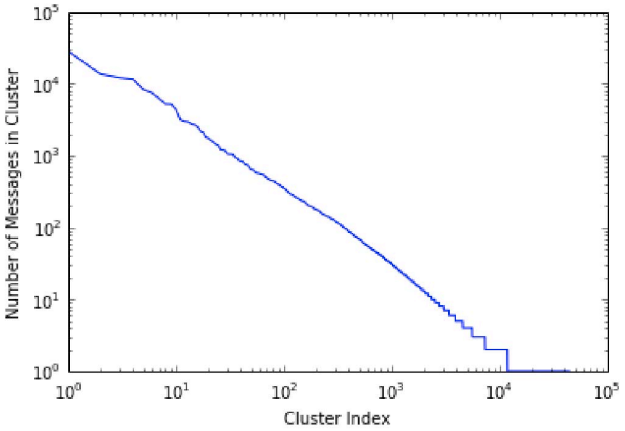


Fig. 2: Cluster sizes are exponentially distributed, and so appear as a straight line when sorted and plotted on a log-log scale.

Tag	Messages	% Tagged
otp-dev	95685	33.4%
code	52872	18.5%
ver	52181	18.2%
conf	38521	13.4%
otp	21919	7.6%
pw-reset	3602	1.3%
ver-url	3139	1.1%
advertising	2999	1.0%
pw-reset-url	2696	0.9%
test	2612	0.9%
info	2339	0.8%
otp-dev-url	863	0.3%
password	697	0.2%
code-url	676	0.2%
conf-ro	401	0.1%
otp-url	320	0.1%
stop	284	0.1%
username	178	0.06%
conf-url	92	0.03%

TABLE IV: We separated and labeled each cluster containing a `code` the intent of the message. This table contains each of those labels and the number of messages in each, which total 74.2% of the messages in our dataset.

5) SMS Usage: As shown in Table IV, messages containing a `code` constitute the majority of our dataset at 67.6% of the total messages, enforcing that a main usage of SMS in our data is verification and authentication.[9] Account creation and mobile device binding `codes` are the largest subcategories

[9]As we note in the previous section, these percentages are reflective of gateway messages, and may not necessarily be representative of broader SMS trends.

with 51.6% of the messages. Compared to other messages containing a `code`, one-time password messages are only 7.6% of messages. The URL variations for these `code` messages are also rare, constituting only 2.6% of messages. This reflects that most services prefer to plain codes, instead of URLs, which may not work well for older phones.

Password reset messages comprise 1.3% of our dataset. The corresponding URL version takes another 1.0% of our dataset. Interestingly, these password reset URLs overwhelmingly consist of Facebook results.

A small part (0.8%) consists of "test" messages. These are messages that consist of text such as "Test," "Hello," or "Hi" with no other information. This category consists of large clusters of messages sent by individuals to probe that the service works as advertised and is currently working. The sender phone numbers, therefore, provide insight into users of the gateways. We explore this more fully later in Section VI.

Finally, a few messages contain partial or complete usernames and passwords. These messages are particularly egregious because they may lead to account compromise and/or user identification. We discuss this further below.

V. Uses of SMS as a Secure Channel

In this section, we discuss what we observed about the security implications if any of the components of the SMS ecosystem described in Figure 1 are compromised. Although the usage we discuss in this section is benign, we observe the presence of PII and low `code` entropy, which are dangerous when available to an adversary in this ecosystem.

A. PII and other Sensitive Information

SMS has become a major portion of global telecommunications worldwide, and its use by companies and other organizations comes as unsurprising. However, our dataset contained instances of companies using SMS to distribute payment credentials or other financial information, login credentials, and other personally identifiable information. We also see instances where gateways are used for sensitive services.

a) Financial information: We found several distinct instances of credit card numbers being distributed over SMS in our dataset. Two of these appear to be intentional methods of distributing new cards, while another two appear to be the result of commerce. We discovered these using PII regular expressions. We also discovered several instances of CVV2 codes in our data. CVV2 codes are credit card codes meant to verify that the user is in possession of the physical card at the time of purchase.

We found that two services that provide "virtual" credit card numbers to allow access to mobile wallet funds distribute the numbers over SMS. These card numbers are "virtual" in the sense that they are not backed by a credit line, but in fact seem to be persistent. The first service is Paytoo, based in the United States. We recovered three distinct cards from this service, and additional messages containing balance updates, account numbers and transaction identifiers. While password reset was handled over email, identifiers such as email, username, phone number, or account number could all be used for login.

The other service is iCashCard, based in India. They distribute a prepaid credit card account number over SMS; this card is protected by a PIN also distributed over SMS. Additional messages contained a separate PIN which allows for account login with the phone number, meaning that access to SMS reveals access to the entire payment credential and account.

We found an additional credit card number, CVV, and expiration value from an unnamed service whose identity or purpose we could not identify. The message indicated that it was being sent to a user who had purchased a "package" of some sort, and confirmed the purchase using the full credit card number. Incidentally, the purchaser's IP address was listed in the SMS, and that IP address was placed in SANS blocklist for suspected bots and forum spammers.

Our PII regular expressions discovered one final credit card number present in a text message sent to a Mexican phone number. The message contains a reference to a Venezuelan bank, the card holder's name, and includes the credit card number, the CVV2, and the expiration date. To determine the context for this message, we examined other messages from this sender and found what appeared to be an SMS-based mailing list for purchasing items on the black market in Venezuela; items for sale included US paper products (diapers, tissue), oil, and tires, as well as US dollars at non-official rates [34]. Our best hypothesis for the presence of the credit card is that a purchaser of an item mistakenly sent payment information to the list in place of the actual sender. Nevertheless, this highlights that highly sensitive enterprises rely on SMS.

In addition to credit card information, we discovered one unidentified Polish service that includes a CVV2 code in their messages after registering for a prepaid service. Translated (by Google), these messages read:

```
Thank you for registering on the
site prepaid. Your CVV2 code is: 194
```

The financial information in our gateway data is not limited to credit card numbers. We found several instances of messages sent by a prepaid credit card provider in Germany, PayCenter [13], that distributes bank account numbers (IBANs) in SMS messages. The same provider also sends a verification text to the user with a URL that includes the user's full name.

The messages above indicate that some services unwisely transmit sensitive financial information over SMS.

b) Usernames and Passwords: In scanning our labeled clusters, we identified several services that would allow user accounts to be compromised if SMS confidentiality is lost. The most prominent example of these is Canadian international calling provider Boss Revolution [2]. Their user passwords are distributed via SMS, and usernames are simply the user's phone number. Thus, an attacker with read access to these messages can compromise an account. Another example was the Frim messaging service [5]. That service also uses the

user's phone number and a password distributed over SMS. Other services distributing usernames and passwords in SMS include eCall.ch (a Swiss VoIP provider) [4] and RedOxygen (a bulk SMS provider) [17]. Fortunately for users, most online services in our data do not distribute password information through SMS.

c) Password Reset: Several organizations, including Facebook and the investment platform xCFD, distribute password reset information via SMS in addition to or in place of other methods. The most common password request in our data was for Facebook account resets. Upon investigating these messages (using only our own accounts), we found that the messages contained a URL that would allow a password reset with no other identifying information or authentication — not even a name or username. This would allow any adversary with access to the message — either as it transits carrier networks, the receiving device, or any other entity that handles the message – to control the account. If the adversary has the username, he/she could cause reset messages to be sent for that account, allowing the adversary to take complete control of the account. This highlights the consequences of a compromise of the SMS ecosystem.

d) Other personally identifiable information: We found numerous examples of PII — including addresses, zip codes, and email addresses. Email addresses are worth noting because the presence of an email address indicating an association between a phone number an account could be used to associate `codes` or other authenticators sent to that device to the particular account. Our PII regular expressions identified 522 messages with emails – most of these were sent by `live.com`, `gmail.com`, `inbox.ru`, or `pop.co` (a hosting provider).

e) SMS Activity from Sensitive Applications: Finally, we noticed several instances where messages appeared in the gateway from organizations whose very nature is sensitive. The worst among these was the roomsharing service Airbnb. One of our messages contained the full address of the shared property (personal information obscured):

```
Airbnb reservation reminder:
Jan 25-28 @ <address>.
<name>: <email> or <phone>
```

Although we suspect that the owner of the property listed it in such a way that this data was revealed, the use of SMS gateways for these services is troubling as it could facilitate real-world abuses.

Other examples of sensitive applications include a large set of registrations with other telecommunications services. These include popular phone services like Telegram, Viber, Line, Burner and Frim. The presence of these services in gateway data may indicate the use of these gateways for "number chaining," a practice that allows PVA evaders to acquire a large number of telephone numbers for free [73]. In addition, we see registration and activity in the gateway data to a number of bulk SMS services. This may indicate the use of gateway numbers to obtain access to bulk SMS services for the purposes of sending SPAM, in addition to a potential use for number chaining.

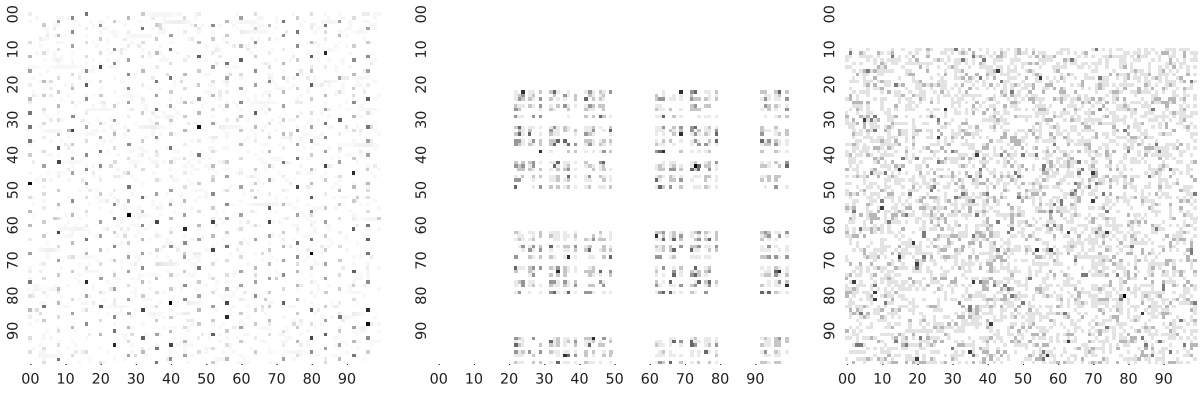
f) Case Study: QIWI Wallet: We have identified one service that uses most of the previously discussed problematic SMS practices: QIWI wallet, a Russian mobile wallet operated in partnership with VISA [23]. First, QIWI wallet sends email addresses in messages to bind emails to accounts. Second, this service also sends password reset codes over SMS, while allowing login with the user's phone number — meaning any reader of the message can reset the user's password. QIWI also provides VISA numbers for its users, and they send partially-blinded card numbers and full CVV2 numbers through SMS. Such partially-blinded information can still be sensitive as knowing the last four digits of a credit card is sometimes used for over-the-phone authentication, and such information has been used in the past to target call centers [45]. More worrisome, they seem to use two different blinding schemes – sometimes blocking the first and last four digits, other times blocking the middle 8 digits of the card. If both blinding schemes are used for the same card, it would be possible to acquire all card information over SMS. This service also sends balance updates over SMS, which are also sometimes used for caller authentication. Finally, we found at least one message in our data corresponding to a QIWI blocked account notification; one possible reason for this is the use of the QIWI account (registered with the gateway number) for fraud or abuse.

B. SMS `code` Entropy

Our message dataset afforded us samples of `codes` sent by many services over SMS. These `codes` provide valuable phone verification capabilities to services that wish to increase the burden of obtaining an account (e.g., to prevent fraudulent account creation), and these `codes` provide a glimpse into the security of the code-generation schemes. We grouped those clusters containing codes by service and extracted the numeric `code` from each message. Overall, we extracted from 33 clusters containing 35,942 authentication codes across 25 services, as shown in Table V.

We first tested the entropy of each set of `codes` using a chi-square test. The chi-square test is a null hypothesis significance test, and in our use case indicates if the `codes` are uniformly generated between the lowest and highest value. The p-value less than 0.01 means that there is a statistically significant difference between the observed data and an ideal uniform distribution. Only 12 of 34 clusters (35%) had p-values > 0.05. We also measure the effect size for each test, finding that most effect sizes were large ($w > 0.5$) with only one medium ($w > 0.3$), indicating our statistically significant differences were in fact meaningful. Finally, we confirmed that all tests performed had a statistical power of 0.98 or higher, indicating that our test had a high likelihood of observing any effect present.

Of the clusters, those belonging to the WeChat and Talk2 services had the least entropy of the authentication `codes` we analyzed. Not only did both services have p-values of 0.0 in



(a) WeChat (b) Talk2 (c) LINE

Fig. 3: These figures present heatmaps of codes where the first two digits are represented on the y-axis and the last two digits are represented on the x-axis. Darker values represent higher frequencies of a code in our data. These figures show that WeChat and Talk2 present an egregious lack of entropy in their authentication codes, while Line generates random codes without leading zeros.

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

TABLE V: The results of our statistical analysis of authentication codes from each service. Some services appear more than once in the data because their messages were split into multiple clusters (e.g., one for password resets and one for logins).

the above chi-square test, the service's codes each generate a specific pattern. We mapped the first two digits of each code with the back two digits and show these two services' codes in Figure 3.

WeChat. Until April 2015, WeChat's authentication codes followed a pattern of $rand() * 16 \mod 10000$, which caused the stair-step offset-by-16 heatmap in Figure 3a. The pattern could be explained by a random number generator with low entropy in the four least significant bits. This effectively reduced the possible space of 4-digit codes to 625. In April 2015, WeChat changed its code generation algorithm. We removed the 625 known-pattern codes from the WeChat set and recomputed the chi-square entropy test. The p-value increased to 0.761 with statistical power and effect size of 0.989 and 0.423, respectively, indicating that the new algorithm is likely producing uniformly-random codes.

Talk2. This service has an extreme lack of entropy in its code-generation algorithm, as seen in Figure 3b. In particular, it appears to avoid digits 0, 1, 2, 5, and 8 in positions 1 and 3 of a 4-digit code. We made several attempts to reproduce this entropy pattern, but we were unable to produce a reasonable explanation for this dramatic reduction in entropy.

Google. While the Google codes we harvested did not appear to be uniformly-random in our experiments, this appears to be caused by duplicate codes. When requesting that a code be resent, Google will send the same code again. This practice is potentially problematic because it indicates that the Google codes have a long lifetime. Since messages on gateways may be accessible for weeks or months, it may be possible for an adversary that can identify the associated account to use an unclaimed code. Without access to the associated accounts, however, we were unable to determine the exact lifetime of Google's codes.

LINE. Although our experiments show LINE's codes are

likely uniformly generated, the service does not generate `codes` with a leading zero, reducing the overall space of `codes` by 10%. This practice is common among our clusters, with 13 total clusters exhibiting this behavior. For comparison, we display LINE's `codes` in Figure 3c.

C. Takeaways

In this section, we explored the data that is exposed in the SMS channel for benign purposes. This is problematic if an adversary has access to SMS messages, as is the case with the gateways. We observed services that expose sensitive user data via SMS including financial data, account information, password reset URLs, and personal information such as physical and e-mail addresses. We then found that 65% of services that use SMS to deliver `codes` generate low-entropy `codes`, which may be predictable and grant unauthorized access to accounts. The design of such services is guided by an assumption that the SMS channel is secure from external observation, and our observations show that this results in poor security design in those applications.

VI. Abuses of SMS

Having explored how services attempt to use SMS as a secure channel, we now discuss what we observed about the security implications and evidence of abuse related to gateway activity. This includes phone verified account evasion, failed attempts at location anonymity, whether similar gateway numbers can be detected, and spam and fraud in the messages themselves.

A. Gateways and PVA

In this subsection, we discuss the relevance of our data to phone-verified accounts. In particular, we present evidence that the primary activity of the gateways we observe is evading phone verified account restrictions, and that existing countermeasures are ineffective.

g) Message Activity Statistics: In Section IV, we noted that more than half of the messages received by gateways are related to account verification. This vastly outweighed any other purpose of sending SMS. Beyond this information, message activity statistics also support this claim. The median number lifetime (the time from first message to last) in our dataset is 20 days, and the CDF of number lifetime is shown in Figure 4a. This lifetime is fairly short, and in fact 73.9% of numbers do not even last a full billing cycle (31 days).

There are two likely explanations for the short lifetime: one is that services that facilitate PVA need to replace their numbers often as they exhaust their usefulness to create new accounts. The second is that many of these numbers are in carriers (especially mobile carriers) that shut off numbers for anomalous message volume. These explanations are not necessarily mutually exclusive.

To gain insight onto this question, we computed the daily volume of messages for each phone number used by a gateway, and we call this series the "daily activity" of the number. If these numbers were being primarily for personal messages or informational activities (like signing up for advertising alerts), we would expect the daily activity of the number to be fairly constant across the lifetime of the number, or for there to be a "ramp up" period as new users discover the new line.

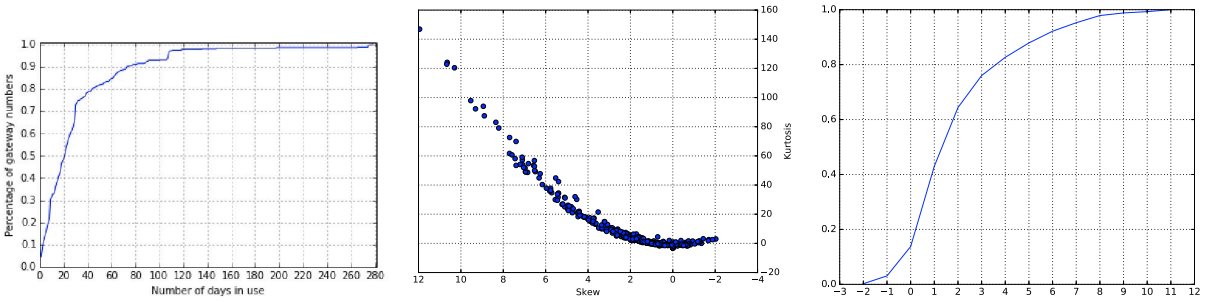
Instead, we see almost the exact opposite behavior. To concisely express this, we computed skewness and kurtosis statistics of the daily activity of every number. Simply, kurtosis is a statistic that indicates if a series is "flat" or "peaky," while skewness indicates whether a peak falls closer to the middle, beginning, or end of a series. A skew of between $(-1, 1)$ indicates the peak falls in the middle of the series, while a positive skew indicates a peak that arrives "earlier" in the series. We plot the skewness and kurtosis for every number in Figure 4b. Note that we reverse the x-axis, so that the further left in the plot a number falls, the "earlier" its peak.

Figure 4c shows the CDF of the daily activity skew, and we observe that approximately 60% of numbers have a skew towards early activity. This implies that most numbers have a high message volume early in the lifetime, and consequently, most of the activity of the number has been completed by the time it is shut down. If carriers are disabling numbers (for exceeding a message rate cap, for example), they are doing so well after most numbers have seen their peak use. Likewise, if online services are considering a number invalid for phone verification, they are still permitting a high-volume of registration requests for a number (in aggregate) before blacklisting the number.

h) User Location Leakage: Some gateways advertise their services towards users that may be seeking privacy or anonymity. Although SMS does not provide either of these properties, the use of a gateway may provide a sense of anonymity for a user registering for a service. Shortened URLs (often provided in space-constrained SMS messages) leak information about the user clicking the link to the URL-shortening service. With the statistics we collected from these services, we have identified both the source and destination countries for each message, we also found that the *users* of these services are located in significantly different locations. *We do not attempt to deanonymize, track, or identify any users.* Our data consists solely of publicly-available aggregate click statistics.

The number of clicks recorded ranged from 0–1,582,634 with a median of 10. This data represents *any* click to these URLs, not just those from the gateway pages. As a result, to prevent skewing our data with popular and spam messages, we focused on URLs with ≤ 10 clicks, since many incoming links expected by users of SMS gateways are likely clicked a small number of times. We collected the countries associated with each of the remaining 2,897 clicks and aggregated the results. Figure 5c shows the total clicks for each country across all shortened URLs. 194 clicks could not be mapped because the specific country information was not available or the service identified that the request was from an anonymizing proxy service.

Also in our data were "test" messages sent by users testing the services. These messages provide another window into



(a) CDF: Number Lifetime (b) Daily Activity Skew and Kurt (c) CDF: Daily Activity Skew

Fig. 4: (a) Only 25% of gateway-controlled numbers are used after one month. The median number lifetime is only 20 days. (b) The skew and kurtosis of number lifetime indicates that 60% of messages have a significant skew towards heavier use at the beginning of the lifetime, while the kurtosis indicates that these numbers see a sharp increase in activity followed by steep decline. (c) 60% of numbers used show a strong tendency for heavy use in the early lifetime of the number.

the user base. Figure 5b and Table XI in the appendix show that the geographical extent of these users goes well beyond the home countries of gateway numbers. Users of gateways may not be aware that these URLs and messages are leaking metadata, and gateways do not adequately warn users of this danger. We consider the use of a gateway as an anonymizing service to be a subset of PVA evasion, however, because users are attempting to evade phone verification, albeit for a different intent.

B. Detecting Gateways

As we have discussed above, these gateways facilitate PVA evasion and the demographic data we can obtain about the users of these services clearly shows usage patterns consistent with PVA fraud. It is clear that in most cases even reputable well-funded online services are not successfully defending against these (and similarly, for-pay gateways). Although number lifetimes are short, the sheer volume of verification messages in our data indicates that evasion is still an effective driver of profit for gateways.

PVA evasion is not new to online services. In particular, Google is acutely aware of this problem, having published a paper on the topic [72]. In that paper, Thomas et al. propose several strategies to detect PVA evasion. They include blocking irreputable carriers, restricting how quickly numbers can verify accounts, and phone re-verification. In this section we explore the recommendations in [72] and discuss how our data shows that *these recommendations are unlikely to be effective*:

Carrier Reputation. While we only see one of the carriers identified as abuse-prone in [72] (`bandwidth.com`), blacklisting blocks of numbers by carrier would not stop all PVA evasion. Carrier-based blocking is prohibitively expensive for all but the largest of organizations. We obtained Twilio data for each number in our data set and although the cost was relatively small ($0.005/lookup), scaling this (and additional number metadata such as CNAM and HLR data) to cover all of a business's customers represents a substantial cost. Furthermore, this kind of bulk blacklisting is difficult to enforce in the face of gateway services that maintain a large pool of numbers over many carriers. Online services that attempt to restrict the speed at which numbers can be reused for new accounts face an arms race against gateways.

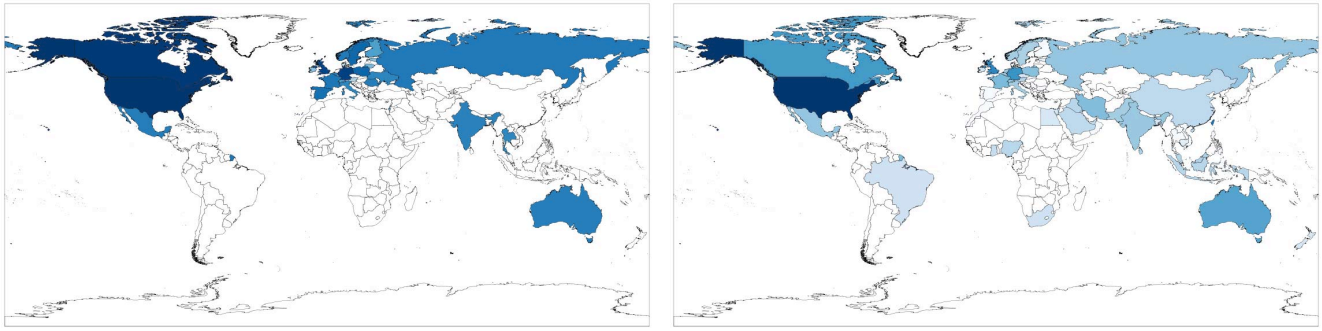
Phone Reputation. One option suggested in [72] for determining phone reputation is to create a service which shares abuse data between service providers. Although little information about how such a service could be created, we considered that it might be possible to blacklist abusive numbers if they are similar to each other.

We conducted a self-similarity analysis against the phone numbers in our dataset to determine how numbers are purchased. If they are purchased in bulk, it may be possible to detect them. We analyzed all of the gateways' numbers to determine similar numbers using Hamming distance. We found that most carriers use similar numbers (i.e., those with a Hamming distance of 2 or less), and the results are shown in Table VI. Over 40% of all of a gateway's numbers were similar in 7 of 8 gateways, however we found that most of these repeated numbers are in *mobile* carriers, not VoIP, as shown in Table VII. The data shows that the gateway numbers are in the carriers that are most likely to serve legitimate users, so attempting to block these numbers may result in a high false positive rate.

Phone Re-verification. Phone number re-verification would fail if the number were checked again outside the expected lifetime of a gateway number. In [72], Thomas et al. saw a median number lifetime of one hour, a reasonable point to perform a re-verification. In our dataset, however, we have seen that half of all gateway numbers last *up to 20 days*. Therefore, re-verification at any interval is unlikely to be universally effective since phone number longevity is not guaranteed.

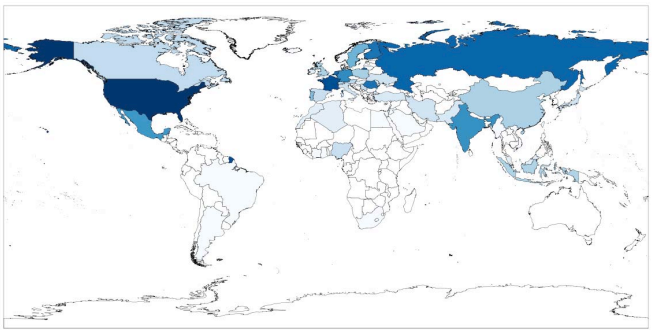
C. Abuse Campaigns in SMS

Since gateways accept unsolicited messages, often do not filter messages, and are subject to users providing these numbers to various services, our data contains SMS from



(a) `Total Messages by Country`

(b) `Test Messages by Country`



(c) `URL Clicks by Country`

Fig. 5: These maps visualize the sender phone number locations of all messages (a) and test messages (b) sent to the gateways. In (c), we map the locations of users that have clicked Bitly- or Google-shortened URLs. These locations provide insight on both the services users are attempting to access and the gateway users themselves. Overall, the locations of the gateways' users significantly differs from the services sending messages, implying the primary purpose of these gateways is PVA fraud.

Site	Similar / Total	Percent
[1] receive-sms-online.info	15 / 59	25.4%
[2] receivesmsonline.net	16 / 38	42.1%
[3] e-receivesms.com	7 / 14	50.0%
[4] hs3x.com	28 / 57	49.1%
[5] receivefreesms.com	52 / 93	55.9%
[6] receivesmsonline.com	38 / 93	40.9%
[7] receive-sms-online.com	8 / 19	42.1%
[8] receive-sms-now.com	20 / 48	41.7%

TABLE VI: We analyzed the numbers from each gateway for similarity. In 7 of 8 gateways, at least 40% of the gateways' numbers were similar.

Carrier Type	Similar / Total	Percent
Mobile	159 / 184	86.4%
Landline	5 / 184	2.7%
VoIP	20 / 184	10.9%

TABLE VII: An analysis of the similarity of gateway numbers shows that the majority of numbers are in mobile carrier number blocks, not VoIP as we expected. As a result, attempting to block these number blocks may result in high false positives.

SPAM campaigns, phishing campaigns, and even one black market as discussed in Section V-A. In this section, we will discuss these campaigns.

1) Spam Campaigns: We found 1.0% of tagged messages across 32 clusters related to advertising. Upon manual inspection none of these appeared to be solicited messages, so we consider these to be spam messages. Of the advertising clusters we identified, 15 are UK-based financial services (e.g., payday loans, credit lines) from 14 numbers. Five are for distinct bulk messaging services. These services advertise gateways and the ability to avoid phone verification: "Using our service to create and verify accounts without your own phone number."

Another six clusters are from a specific job staffing site and appear to be bulk messages related to a job search. Curiously, these messages contain a name and zip code. We expanded the search beyond the labeled clusters and found 282 messages in 107 clusters. These messages may be related to this organization testing their bulk SMS API. All of these messages were sent to a single gateway number within a seven-hour timespan, which is unusual when compared to other bulk message campaigns in our dataset. Finally, two of these messages have links to surveys via Bitly links. These links were created by user "smsautodialer", who has been a member since July 2015 and has shared over 2,802 Bitly links. The destination domain has a 0/65 detection ratio on VirusTotal.

We were surprised at the low spam volume observed in public gateways, as they market themselves as a service for

Domain	Sender MSISDN	Time to First Message
danske-mobile*com	DanskeBank	0 days 11:41:02
location-message*com	243858234346	0 days 13:38:02
it-panels*com	16312237715	0 days 16:30:02
iurl-sms*com	14156537352	0 days 16:30:02
phone-gps*com	243858214490	0 days 18:41:03
url-sms*com	243858361940	0 days 18:47:03
location-device*com	243858097749	0 days 19:42:02
sms-new-page*com	243858289642	0 days 20:08:02

TABLE VIII: Using domain WHOIS information, we measured the distance between the time a domain was first registered and the time a gateway first received a message containing a URL with this domain. In total, 8 domains appeared in messages within 24 hours of being registered.

avoiding spam. This has been a major topic of research, but the volume of spam traffic in our dataset is lower than previously measured [37], [65].

2) Phishing Campaigns: In contrast to spam, phishing messages attempt to trick the user into believing he/she is communicating with a legitimate entity (e.g., to steal service credentials). These scams typically use "fast-flux" domain registrations to defeat domain blacklisting strategies. Therefore, the age of the domain at the time a message arrives containing that domain is of particular value; if the domain is new, it may indicate that the domain is malicious. We matched the timestamps for incoming SMS messages with the registration times for the domains included in each message.

The fastest domain to appear in our dataset was `danske-mobile*com`,[10] a domain that had been registered for only 11 hours before it appeared in an SMS message. The text of the message (translated from German) is *"Dear Danske Bank customer, you have received an internal message"* alongside the URL. We believe this to be a banking phishing message, however we were unable to verify the URL's purpose. At the time of this writing, the specific host in the message returns a DNS `NXDOMAIN` error and the second-level domain returns a registrar parking page. The SMS gateway that received this message did not display the sender MSISDN number, instead replacing it with "DanskeBank," which may indicate number spoofing. Curiously, the domain WHOIS data shows detailed personal information (name, address, phone number) of the registrant, who is based in the United States. The real Danske Bank web site has registration data with contact information in its home country, Denmark. Given this domain's intended purpose, we believe that this data is either incorrect or stolen personal information, and we did not pursue the ownership further.

In total, 8 domains appeared in messages after being registered for less than one day, as shown in Table VIII. Only one of these domains was accessible via HTTP at the time of writing. The domain, `phone-gps*com`, has an error and delivers a stack trace when no HTTP user-agent string is provided; when we provided one, it delivers empty content (0 bytes). This site, therefore, may be using user-agent strings to determine what content to deliver, however we were not able to get the site to deliver any content with common strings for desktop and mobile browsers. The remaining 7 domains are all registered with contact addresses and registrars based in China and take the form of hyphen-separated English words. Since none of these domains had accessible hosts at the time of writing, we were unable to determine their purpose.

[10]We substitute an asterisk into suspicious URLs in this paper to prevent PDF readers from inferring hyperlinks.

```
Apple Customer,
Your lost iPhone has been found \
    and temporarily switched ON.
To view iPhone map location
lostandfounds-icloud*com
Apple
```

Fig. 6: The phishing SMS message, as received by a gateway. This message is the first step to deceiving a user into providing his/her Apple ID credentials. We substituted the asterisk in to prevent accidental clicks.

Since we were unable to verify the intent of the above domains, we manually searched our dataset for a recently-seen newly-registered domain. We found `lostandfounds-icloud*com`, a site that is designed to appear like the legitimate "Find My iPhone" Apple service. Figure 6 shows the SMS message containing this URL, which also indicates a phishing attempt.

The page's code appears to reject any user name or password entered into the fields (a common practice among phishing sites), and indeed, upon putting any content in these fields, the page returned the error seen in Figure 7. As of November 2015 (less than one month since the message arrived at the gateway), the site has been taken offline. Due to the necessity of retrieving working domains from newly-obtained messages, this message appears later in our dataset than other messages we discuss in this paper.

3) Other malicious behavior: Another empirical measure of the maliciousness of the URLs is scanning these URLs with security products. VirusTotal provides one such measure by requesting scans from multiple products. The full results are displayed in Table IX. VirusTotal returned 417 URLs with at least one detection. Only 3 URLs had 5 detections, and no URL had more than 5 detections. Of these detections, 508 were detected as "malicious site," 147 as "malware site," and 25 as "phishing site." Unsurprisingly, `danske-mobile*com` was not detected by any product, since this domain no longer appears to host any content and it is unlikely that any of these products can determine phishing attempts using the metadata we previously discussed.

Overall, abusive messages (spam, phishing, and malware) consisted of only a small portion of our dataset, despite being billed as a major problem in popular press. This is especially strange given that evasion of spam is something many of the gateways advertise, as we discussed in Section III. Given previous reports on the pervasiveness of SMS spam, we believe that some entity in the SMS ecosystem is performing adequate

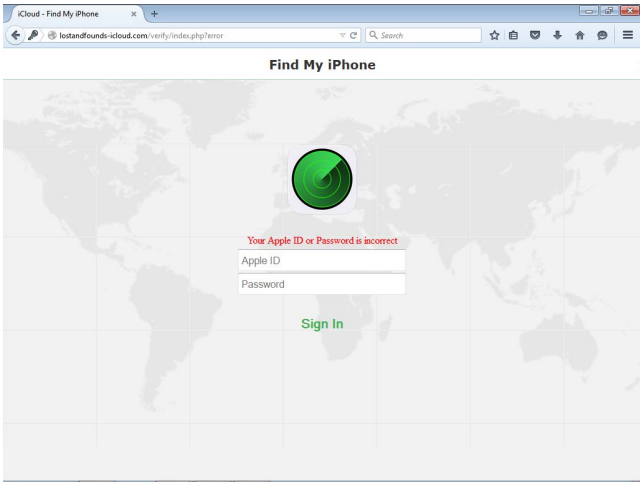


Fig. 7: The page delivered to the user after following a link provided in a phishing SMS. The site refuses any username and password combination provided and displays the error shown in this figure.

spam filtering and that this problem may no longer be as severe as it once was.

D. Takeaways

In this section, we explored malicious uses of the SMS channel. First, we discussed how our data shows the prevalence of PVA evasion due to the stark contrast between gateway number locations and locations of users interacting with the gateways. We then discussed the difficulty of detecting gateways with carrier blocking due to cost and number lifetimes. Finally, we explored abuse campaigns via SMS and found that spam, phishing, and suspicious URLs are infrequent, which may indicate that SMS filtering at the gateways and in the network are sufficient.

VII. Related Work

Prior measurement work has studied the underground economies [71] that drive spam [47], [48], [73], malware [33], [44], [68] and mobile malware [41], [55], [83], and other malicious behavior. While others have investigated SMS content and metadata in the context of SMS spam [46], [60], [61], [75], this work is the first to expansively measure how SMS is used for security purposes by legitimate services. We note that much of the research in this area has been forced to rely on small datasets (some less than 2000 messages [61]). Mobile two-factor authentication is increasing in popularity, with some eagerly heralding its arrival [27] and others cautioning that it may only provide a limited increase in security [63]. Much of the data we collected contained mobile two-factor authentication tokens sent over SMS. While SMS tokens are popular in many contexts, including mobile banking and finance [62], other approaches have been implemented in a variety of forms including keychain fobs [7], [18], one-time pads [56], [64], biometric scanners [31], [67], and mobile phones [10], [26],

Product	Detections
ADMINUSLabs	1
AutoShun	144
Avira	7
BitDefender	15
Blueliv	5
C-SIRT	1
CLEAN MX	11
CRDF	5
Dr.Web	62
ESET	6
Emsisoft	23
Fortinet	31
Google Safebrowsing	15
Kaspersky	3
Malekal	3
Malware Domain Blocklist	20
Malwarebytes hpHosts	1
ParetoLogic	54
Phishtank	1
Quttera	2
SCUMWARE.org	4
Sophos	28
Spam404	3
Sucuri SiteCheck	94
TrendMicro	1
Trustwave	55
Web Security Guard	1
Websense ThreatSeeker	81
Webutation	2
Yandex Safebrowsing	1

TABLE IX: We requested VirusTotal scans for each extracted URL in our dataset. This table shows the number of detections for each product that detected a malicious URL. Overall 417 URLs had at least one detection.

[36]. Analysis of individual systems has led to the discovery of a number of weaknesses, including usability concerns [24] and susceptibility to desktop [50] or mobile malware [32], [38], [40], [49], [51], [59]. SMS-based tokens are especially vulnerable to link-layer attacks against the cellular network. These networks use vulnerable channel encryption [28], [29], [39], allow end devices to connect to illicit base stations [25], [35], [43], and are vulnerable to low-rate denial of service attacks [77], [78]. However, the majority of the infrastructure behind many two-factor authentication systems — the portions of the system outside the cellular network — has not been previously explored from a security perspective.

Dmitrienko et al. were the first to examine SMS messages to study security of two-factor authentication schemes [38]. We greatly exceed the scope of their work in five important ways. First, our work presents a cohesive examination of the entire SMS infrastructure — from online services to end devices. Second, we focus on how online services use SMS well beyond two-factor authentication. Third, our data includes two orders of magnitude more services and we identify and classify the intent of each message. Fourth, we provide a more detailed classification of two-factor authentication systems. Finally, our more rigorous entropy analysis of two-factor authentication PINs allow us to make strong claims for more than 30 services (instead of just 3), helping us to find egregious entropy problems in the popular WeChat and Talk2 services.

Our emphasis on phone verified accounts provides a separate contribution. Thomas et al. study the effects of phone verified accounts at Google [72]. While they use datasets of purchased or disabled PVAs, we provide insight into PVA fraud from enabling services. While we confirm some of their observations, our data indicated their recommendations may prove ineffective at defeating PVA evasion.

VIII. Conclusions

Text messaging has become an important part of the security infrastructure. However, this ecosystem has evolved significantly since its inception, and now includes a wide range of devices and participants external to traditional cellular providers. Public SMS gateways directly embody this change, and allow us to not only observe at scale how a range of providers are implementing security solutions via text messages, but also provide us evidence of how assumptions about SMS are being circumvented in the wild. While our data may not fully encompass all communications sent over SMS, our measurements identify a range of popular services whose one-time messaging mechanisms should be improved, and additional entities who may be creating new opportunities for compromise by sending highly sensitive data (e.g., credit card numbers) via these channels. On the abuse side, we see the ease with which these gateways are being used to circumvent authentication mechanisms, and show that previously proposed mitigations to PVA fraud such as block banning are unlikely to be successful in practice. These measurements indicate that all providers relying on SMS as an out of band channel for authentication with strong ties to a user's identity should reevaluate their current solutions for this evolving space.

Acknowledgments

The authors are grateful to our shepherd, Emin Gün Sirer, and our anonymous reviewers for their helpful guidance. The authors would like to thank Twilio for their generous access to their data and Benjamin Mood for providing considerable assistance formatting our tables and figures. This work was supported in part by the US National Science Foundation under grant numbers CNS-1526718, CNS-1464087, CNS-1540217, CNS-1542018, and CNS-1464088. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Apple continuity. https://support.apple.com/en-us/HT204681.
[2] Boss Revolution. https://www.bossrevolution.ca.
[3] Burner app. http://www.burnerapp.com.
[4] eCall. http://www.ecall.ch.
[5] Frim. http://fr.im.
[6] Google voice. http://www.google.com/voice.
[7] IdentityGuard Identity Authentication Platform. https://www.entrust.com/products/entrust-identityguard/.
[8] LiqPay. https://www.liqpay.com.
[9] Mightytext. http://mightytext.net.
[10] Mobile Authentication. https://www.duosecurity.com/product/methods/duo-mobile.
[11] Nexmo. https://www.nexmo.com/.
[12] OpenCNAM. https://www.opencnam.com.
[13] PayCenter. https://www.paycenter.de.
[14] Pinger. http://www.pinger.com.
[15] Plivo. https://www.plivo.com/.
[16] Pushbullet. http://pushbullet.com.
[17] RedOxygen. http://www.redoxygen.com.
[18] RSA SecurID Hardware Tokens. http://www.emc.com/security/rsa-securid/rsa-securid-hardware-tokens.htm.
[19] Scrapy. http://scrapy.org.
[20] SMSGlobal. https://www.smsglobal.com.
[21] Talk2. http://talk2ph.com.
[22] Twilio. http://www.twilio.com.
[23] Visa QIWI Wallet. https://qiwi.ru.
[24] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis. How to Attack Two-Factor Authentication Internet Banking. In *Financial Cryptography and Data Security*, number 7859 in Lecture Notes in Computer Science, pages 322–328. Springer Berlin Heidelberg, Apr. 2013.
[25] Z. Ahmadian, S. Salimi, and A. Salahi. New attacks on UMTS network access. In *Wireless Telecommunications Symposium, 2009. WTS 2009*, pages 1–6, Apr. 2009.
[26] F. Aloul, S. Zahidi, and W. El-Hajj. Two factor authentication using mobile phones. In *IEEE/ACS International Conference on Computer Systems and Applications, 2009. AICCSA 2009*, pages 641–644, May 2009.
[27] J. Atwood. Make Your Email Hacker Proof. http://blog.codinghorror.com/make-your-email-hacker-proof/, Apr. 2012.
[28] E. Barkan, E. Biham, and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. *Journal of Cryptology*, 21(3):392–429, Sept. 2007.
[29] A. Biryukov, A. Shamir, and D. Wagner. Real Time Cryptanalysis of A5/1 on a PC. In *Proceedings of the 7th International Workshop on Fast Software Encryption*, FSE '00, pages 1–18, London, UK, UK, 2001. Springer-Verlag.
[30] K. Campbell-Dollaghan. How Hackers Reportedly Side-Stepped Google's Two-Factor Authentication. http://gizmodo.com/how-hackers-reportedly-side-stepped-gmails-two-factor-a-1653631338, Nov. 2014.
[31] CardTechnology. UAE ID Card To Support Iris Biometrics. http://www.cardtechnology.com/article.html?id=20070423V0XCZ91L, 2007.
[32] C. Castillo. Spitmo vs Zitmo: Banking Trojans Target Android. http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android, Sept. 2011.
[33] C. Y. Cho, J. Caballero, C. Grier, V. Paxson, and D. Song. Insights from the inside: A view of botnet management from infiltration. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2010.
[34] N. Crooks. Venezuela, the Country With Four Exchange Rates. http://www.bloomberg.com/news/articles/2015-02-19/venezuela-the-country-with-four-exchange-rates, Feb. 2015.
[35] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl. IMSI-catch me if you can. In *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014.
[36] D. DeFigueiredo. The Case for Mobile Two-Factor Authentication. *IEEE Security Privacy*, 9(5):81–85, Sept. 2011.
[37] S. J. Delany, M. Buckley, and D. Greene. SMS spam filtering: Methods and data. *Expert Systems with Applications*, 39(10):9899–9908, 2012.
[38] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi. On the (In)Security of Mobile Two-Factor Authentication. In *Financial Cryptography and Data Security (FC14)*. Springer, Mar. 2014.
[39] O. Dunkelman, N. Keller, and A. Shamir. A Practical-time Related-key Attack on the KASUMI Cryptosystem Used in GSM and 3g Telephony. In *Proceedings of the 30th Annual Conference on Advances in Cryptology*, CRYPTO'10, pages 393–410, Berlin, Heidelberg, 2010. Springer-Verlag.
[40] J.-E. L. Eide. *SMS One-Time Passwords: Security in Two-Factor Authenication*. Master's Thesis, University of Bergen, May 2015.
[41] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A Survey of Mobile Malware in the Wild. In *ACM Workshop on Security and Privacy in Mobile Devices*, Chicago, Illinois, USA, Oct. 2011.
[42] B. J. Frey and D. Dueck. Clustering by passing messages between data points. *Science*, 315(5814):972–976, 2007.
[43] N. Golde, K. Redon, and R. Borgaonkar. Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications. In *NDSS*, 2012.

[44] C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, N. Provos, M. Z. Rafique, M. A. Rajab, C. Rossow, K. Thomas, V. Paxson, S. Savage, and G. M. Voelker. Manufacturing Compromise: The Emergence of Exploit-as-a-service. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 821–832, New York, NY, USA, 2012. ACM.

[45] M. Honan. How Apple and Amazon security flaws led to my epic hacking. http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/, Aug. 2012.

[46] N. Jiang, Y. Jin, A. Skudlark, and Z.-L. Zhang. Greystar: Fast and Accurate Detection of SMS Spam Numbers in Large Cellular Networks using Grey Phone Space. In *Proceedings of the 22nd USENIX Security Symposium.*, Washington DC, USA, 2013. USENIX Association.

[47] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 3–14. ACM, 2008.

[48] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. M. Voelker, and S. Savage. Show Me the Money: Characterizing Spam-advertised Revenue. In *USENIX Security Symposium*, pages 15–15, 2011.

[49] R. E. Koenig, P. Locher, and R. Haenni. Attacking the Verification Code Mechanism in the Norwegian Internet Voting System. In J. Heather, S. Schneider, and V. Teague, editors, *E-Voting and Identity*, Lecture Notes in Computer Science, pages 76–92. Springer Berlin Heidelberg, July 2013.

[50] R. K. Konoth, V. van der Veen, and H. Bos. How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. In *Proceedings of the 20th International Conference on Financial Cryptography and Data Security*, 2016.

[51] L. Koot. *Security of mobile TAN on smartphones*. Master's Thesis, Radboud University Nijmegen, Nijmegen, Feb. 2012.

[52] B. Krebs. Banks: Credit Card Breach at Home Depot. http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/, Sept. 2014.

[53] B. Krebs. Experian Breach Affects 15 Million Consumers. http://krebsonsecurity.com/2015/10/experian-breach-affects-15-million-consumers/, Oct. 2015.

[54] B. Krebs. Online Cheating Site AshleyMadison Hacked. http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/, July 2015.

[55] C. Lever, M. Antonakakis, B. Reaves, P. Traynor, and W. Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the 20th Network and Distributed System Security Symposium*, San Diego, CA, Feb. 2013.

[56] J. Leyden. Visa trials PIN payment card to fight online fraud. http://www.theregister.co.uk/2008/11/10/visa_one_time_code_card/, 2008.

[57] H. P. Luhn. Computer for verifying numbers, 1960. US Patent 2,950,048.

[58] E. McCallister, T. Grance, and K. Scarfone. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf, 2010.

[59] C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert. SMS-based one-time passwords: attacks and defense. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 150–159. Springer, 2013.

[60] I. Murynets and R. Piqueras Jover. Crime Scene Investigation: SMS Spam Data Analysis. In *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*, IMC '12, pages 441–452, New York, NY, USA, 2012. ACM.

[61] A. Narayan and P. Saxena. The Curse of 140 Characters: Evaluating the Efficacy of SMS Spam Detection on Android. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM '13, pages 33–42, New York, NY, USA, 2013. ACM.

[62] B. Reaves, N. Scaife, A. Bates, P. Traynor, and K. Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015.

[63] B. Schneier. Two-factor Authentication: Too Little, Too Late. *Commun. ACM*, 48(4), Apr. 2005.

[64] SiPix Imagining, Inc. World's First ISO Compliant Payment DisplayCard using SiPix and SmartDisplayer's Flexible Display Panel. http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20060510006193&newsLang=en, 2006.

[65] A. Skudlark. Characterizing SMS Spam in a Large Cellular Network via Mining Victim Spam Reports, Dec. 2014.

[66] SMS Forum. Short Message Peer to Peer Protocol Specification 5.0, 2003.

[67] A.-B. Stensgaard. Biometric breakthrough - credit cards secured with fingerprint recognition made feasible. http://www.ameinfo.com/58236.html, 2006.

[68] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 635–647, New York, NY, USA, 2009. ACM.

[69] The International Organization for Standardization. ISO 8601 - Time and date format. http://www.iso.org/iso/home/standards/iso8601.htm, 2004.

[70] The Open University. 2014 Text Messaging Usage Statistics. http://www.openuniversity.edu/news/news/2014-text-messaging-usage-statistics, Dec. 2014.

[71] K. Thomas, D. Huang, D. Wang, E. Bursztein, C. Grier, T. J. Holt, C. Kruegel, D. McCoy, S. Savage, and G. Vigna. Framing Dependencies Introduced by Underground Commoditization. In *Proceedings of the 14th Annual Workshop on the Economics of Inforamtion Security*, 2015.

[72] K. Thomas, D. Iatskiv, E. Bursztein, T. Pietraszek, C. Grier, and D. McCoy. Dialing Back Abuse on Phone Verified Accounts. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 465–476, New York, NY, USA, 2014. ACM.

[73] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *USENIX Security*, pages 195–210, 2013.

[74] A. Tims. SIM swap gives fraudsters access-all-areas via your mobile phone. *The Guardian*, Sept. 2015.

[75] H. Toan, N. Goharian, and M. Sherr. $100,000 Prize Jackpot. Call Now!: Identifying the Pertinent Features of SMS Spam. In *Proceedings of the 35th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 1175–1176, New York, NY, USA, 2012. ACM.

[76] P. Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.

[77] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.

[78] P. Traynor, P. McDaniel, and T. La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007.

[79] P. Traynor, P. McDaniel, and T. La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

[80] U.S. Office of Personnel Management. Cybersecurity Incidents. https://www.opm.gov/cybersecurity/cybersecurity-incidents/, 2015.

[81] Vassilis Prevelakis and Diomidis Spinellis. The Athens Affair. *IEEE Spectrum*, June 2007.

[82] VirusTotal. VirusTotal - Free Online Virus, Malware and URL Scanner. https://www.virustotal.com/, 2015.

[83] Y. Zhou and X. Jiang. Dissecting Android Malware: Characterization and Evolution. In *2012 IEEE Symposium on Security and Privacy (SP)*, pages 95 –109, May 2012.

APPENDIX

Carrier	Amount
Mobile	
E Plus Mobilfunk	33
Everything Everywhere (T-Mobile)	23
Hutchison 3G UK	15
Gotalandsnatet	13
Alands Mobiltelefon	13
Telstra Corporation	13
Sure (Guernsey) Limited	10
Tele2 Sverige	9
T-Mobile	8
Vodafone Espana	7
Netia Mobile Sp. z o.o. (P4)	7
Lycamobile	6
BOUYGUES TELECOM	6
Polska Telefonia Cyfrowa Sp. z o.o. (PTC)	5
Nextel Mexico	5
Mobile Norway	5
Cellcom	5
True Move	4
Lleida Networks Serveis Telematics	4
Vodafone	4
TRANSATEL	4
CITIC Telecom 1616	4
Orange Romania	3
Tele2 Norge AS	3
O2 Communications (Ireland) Ltd.	3
Vimpel Communications	3
Belgacom Mobile - Proximus	3
Vodafone Romania	3
China Mobile Hong Kong Co	3
POLKOMTEL S.A.	3
Swisscom	3
Telefonica (O2 Germany GmbH & Co. OHG)	2
MTS Ukraine (Jeans (UMC))	2
Bharti Airtel Ltd	2
Vodafone D2	2
T-Mobile USA, Inc.	1
Telefonica UK	1
Level 3	1
Tele 2 Eesti	1
UAB Tele2	1
Orange	1
Telenor	1
A Telecom	1
Kyivstar	1
T-Mobile Czech Republic	1
Total Access Communication Plc. (TAC/DTAC)	1
Unknown Carrier	12
VoIP	
Twilio	78
Bandwidth SMSEnabled	69
Google (Grand Central) BWI	2
Landline	
Jersey Telecom	5
Sure (Guernsey) Limited	4
Telus Communications Inc.	2

TABLE X: Gateway numbers are placed in a wide variety of carriers.

Country	Message Count	URL Clicks	Test Messages
United States	95138	964	744
Canada	77036	6	56
Germany	53497	95	65
United Kingdom	44039	10	89
Poland	16103	11	17
Sweden	14849	29	9
Spain	11323	5	1
France	8273	478	20
Russian Federation	7344	276	14
Norway	6674	1	11
Mexico	6431	71	14
Romania	6043	190	-
Australia	5964	-	43
Belgium	5253	3	10
India	5064	81	13
Ukraine	4363	4	-
Italy	4326	4	11
Thailand	4073	-	1
Hong Kong	3251	-	13
Israel	1971	6	6
Switzerland	1722	9	14
Finland	1714	191	1
Lithuania	520	1	-
Estonia	405	-	2
Ireland	331	2	3
Austria	158	7	8
Denmark	54	-	-
Czech Republic	6	-	3
Netherlands	-	247	12
Portugal	-	21	1
China	-	10	6
Indonesia	-	9	7
Nigeria	-	5	7
Serbia	-	5	1
Luxembourg	-	5	-
Iran	-	4	18
Japan	-	4	-
Pakistan	-	3	11
Moldova	-	3	-
Turkey	-	3	-
Malaysia	-	2	8
Morocco	-	2	1
Hungary	-	2	-
Algeria	-	2	-
Taiwan	-	1	144
Saudi Arabia	-	1	6
Ghana	-	1	5
Brazil	-	1	4
South Africa	-	1	4
Egypt	-	1	3
Bulgaria	-	1	1
Vietnam	-	1	1
Argentina	-	1	-
Iceland	-	1	-
Ivory Coast	-	1	-
Jordan	-	1	-
Myanmar	-	1	-
Sri Lanka	-	-	9
Iraq	-	-	7
Singapore	-	-	6
United Arab Emirates	-	-	5
Isle of Man	-	-	4
Kuwait	-	-	4
Bangladesh	-	-	3
Lebanon	-	-	3
New Zealand	-	-	3
Cambodia	-	-	2
Costa Rica	-	-	1
Jamaica	-	-	1
Maldives	-	-	1
Oman	-	-	1
Philippines	-	-	1
Reunion Island	-	-	1
Slovakia	-	-	1

TABLE XI: This table contains the counts of the geolocated sender phone numbers for each country alongside the number of URL clicks from users based in those countries and the number of test messages sent to those countries. This data underscores the variation between the users of the gateway services and the numbers sending messages to the gateways.