Identifying Account Association with Assistance from Mobile Networks using Cross-Service Attacks

Sean W. Caldwell, Ye Zhu
Computer Science and Electrical Eng.
Cleveland State University
Cleveland, OH, USA
2595953@vikes.csuohio.edu
y.zhu61@csuohio.edu

Yong Guan
Electrical and Computer Eng.
Iowa State University
Ames, IA, USA
yguan@iastate.edu

Riccardo Bettati
Computer Science and Eng.
Texas A&M University
College Station, TX, USA
bettati@tamu.edu

***Abstract*—In this paper, we draw attention to the problem of cross-service attacks, that is, attacks that exploit information collected about users from one service to launch an attack on the same users on another service. With the increased deployment and use of what fundamentally are integrated-services networks, such as 4G/LTE networks and now 5G, we expect that cross-service attacks will become easier to stage and therefore more prevalent. As running example to illustrate the effectiveness and the potential impact of cross-service attacks we will use the problem of account association in 4G/LTE networks. Account association attacks aim at determining whether a target mobile phone number is associated with a particular online account. The the case of 4G/LTE, the adversary launches the account association attacks by sending SMS messages to the target phone number and analyzing patterns in traffic related to the online account. We evaluate the proposed attacks in both a local 4G/LTE testbed and a major commercial 4G/LTE network. Our extensive experiments show that the proposed attacks can successfully identify account association with close-to-zero false negative and false positive rates. Our experiments also illustrate that the proposed attacks can be launched in a way that the victim receives no indication of being under attack.**

***Index Terms*—SMS, traffic analysis, 4G/LTE**

I. Introduction

In this paper, we study the problem of *cross-service attacks*, that is, attacks that exploit information collected about users from one service to launch an attack on the same users on another service. With the increased deployment and use of what fundamentally are integrated-services networks, such as 4G/LTE networks and now 5G, we expect that cross-service attacks will become easier to stage and therefore more prevalent. As multiple services share the underlying infrastructure, for example SMS and IP services on 4G/LTE, information gathered from one service on the network can disclose information about users of other services.

As running example to illustrate the effectiveness and the potential impact of cross-service attacks we will use the problem of account association in 4G/LTE networks. The goal of account association is to determine whether a target mobile phone number is associated with a particular online account for an IP-based service such as Skype or Netflix. The demand for associating phone numbers with online accounts may emerge in a variety of settings. For example, many smartphone applications and services require users to provide their phone numbers during account registration. If adversaries are able to associate service accounts with the their registered telephone numbers, they may be able to compromise the privacy of the application and that of their users. For example, an adversary may suspect a particular individual of anonymously broadcasting live videos through a smartphone applications such as Periscope. The adversary can infer the identity of the Periscope account owner by associating the account with the owner's phone number.

4G/LTE networks are particularly susceptible to the type of cross-service attacks addressed in this paper because all the services provided by 4G/LTE rely on the same IP-based communication channels. This includes services that one does not traditionally think of as IP based, such as voice calls and SMS messages, and services that are generally built on IP, such as high-definition mobile video, mobile augmented or virtual reality, and mobile cloud computing. We will see that the requirement for 4G/LTE to provide low-delay and high-bandwidth services renders cross-service attacks particularly effective. The opportunities for this type of attack will grow as well. Given the popularity of 4G/LTE and 5G, such attacks will likely become quite prevalent and impactful.

We will study a class of account association attacks specifically designed for the 4G/LTE networks: An adversary initiates the attacks by sending SMS messages to the target phone number and by analyzing the traffic related to the account. If the analysis can find traffic patterns corresponding to the SMS messages, the attack assumes that the target phone number is associated with the account.

We staged a number of attacks within a local 4G/LTE testbed. The results indicate that the proposed attacks can accurately identify account associations. Our local experiments also show that the attacks can be "silent" to the victim, meaning that the victim receives no indication that it is the target of an account association attack. These "silent" attacks are possible because existing smartphones have no abilities to process messages in some specific formats, such as CPIM [1]. We will show that although the victim does not know that a "silent" attack is under way, the proposed attacks can actually achieve better identification performance when CPIM

or similar message formats are being used compared to attacks with user-visible SMS messages.

When deployed in commercial 4G/LTE networks, these attacks in their basic forms are less effective, mainly because the SMS service center and the uplink bandwidth are shared among many service subscribers. The scheduling algorithm used in this sharing tend to spread the SMS messages in order to prevent the batching of SMS messages to any particular subscriber. This makes it hard for the attacker to find the correspondence between the traffic patterns and SMS messages. We describe how an attacker can overcome this challenge by employing a class of attacks that is particularly well suited against commercial 4G/LTE networks. These attacks leverage the knowledge about how spreading and throttling is realized by network operators, and take advantage of the spreading and throttling caused by the scheduling for identification. We evaluate this new class of attacks using an extensive suite of experiments over a major commercial 4G/LTE network. The results illustrate the effectiveness of these attacks and show that one can identify account associations with high accuracy on large commercial 4G/LTE networks.

The success of the proposed account association attacks should encourage us to re-think the architecture of 4G/LTE networks and integrated-services architectures in general. As mobile-network providers transitioned from 3G to 4G/LTE networks, they also transitioned to a fully IP-based underlying platform. As a result, a highly diverse set of services, including voice calls and SMS messages, are now provided over a shared, IP-based network. Integrating these services brings many advantages, such as better scalability and richness of features. It does, however, expose the services to attacks, primarily side-channel attacks, that span individual services. As we will show, such attacks are particularly effective against services that provide Quality-of-Service (QoS) guarantees, such as voice, video, and various forms of augmented or virtual reality services. As a result, attention must be paid as we transition to next-generation architectures for mobile network to the importance of preventing cross-service covert channel attacks, much as the attacks proposed in this paper.

II. Background

1) Network Architecture for 4G/LTE: 4G/LTE networks provide all their services over a flat, all-IP architecture. This is in contrast to the hierarchical structures used in previous architectures. The flat, all-IP architecture of 4G/LTE enables constantly higher bandwidths with significantly lower data-transfer delays compared to those of 2G and 3G networks. In a 4G/LTE network, a *User Equipment* (UE), such as a smartphone, connects to a 4G/LTE network through one of the base stations, also called *Evolved Node B* devices (eNodeB's). The eNodeB devices are elements of the *Evolved Universal Terrestrial Radio Access Network* (E-UTRAN), which is responsible for keeping the UEs wirelessly connected, and which is designed to help improve overall wireless connectivity. The eNodeBs are connected to the *Evolved Packet Core* (EPC), which provides 4G/LTE services to a subscribed UE.

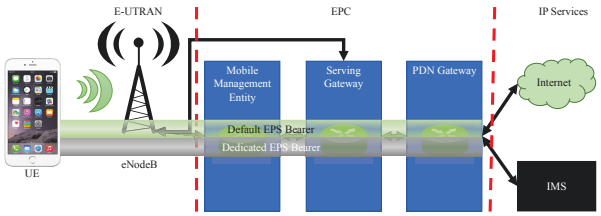


Fig. 1: A Typical Scenario of VoLTE

The EPC consists of the following components: (1) The *Mobile Management Entity* (MME) is responsible for tracking the UE and for providing the initial connection and authentication for the UE device. Particularly important for the proposed attacks is the MME's role in activation and deactivation of *bearers*, which uniquely identify traffic flows with specific Quality of Service (QoS) requirements. Figure 1 shows how two bearers are used in a 4G/LTE network, one for IP traffic and the other for voice. (2) the *Home Subscriber System* (HSS) is a database that maintains user profiles and location information. It acts as a source for name and address resolution and for authentication. (3) The *Serving Gateway* (SGW) is responsible for managing all IP packets that flow through the network. (4) The *Packet Data Network Gateway* (PGW) is responsible for allocating IP addresses to the UEs. It provides an interface towards the Internet and to the *IP Multimedia Subsystem* (IMS), which in turn provides multimedia services, including voice-over-LTE. Particularly related to the proposed attacks is PGW's role in setting up the appropriate bearers to establish the corresponding connections to IMS services. The EPC is – differently than in 2G/3G mobile networks – an *IP-only core network* that supports packet-switching.

2) Voice over LTE: IMS is the current designated solution for offering multimedia services in 4G/LTE mobile networks. It shifts the voice communications of mobile devices from the legacy circuit-switching technology to the packet-switching design used in 4G/LTE. In comparison to 3G networks and even Voice over IP (VoIP), voice-over-LTE (VoLTE) packets have smaller packet headers and therefore save bandwidth [2].

A typical scenario of VoLTE communications is shown in Figure 1. A VoLTE-capable phone is connected to the 4G/LTE network with two bearers. The *default bearer* is established when a UE connects to a 4G/LTE network. It remains established to provide the UE with always-on IP connectivity. The default bearer is typically setup without any QoS requirements. It is primarily used for general IP traffic. A *dedicated bearer* is used for VoLTE communications. The dedicated bearers established for (delay-sensitive) voice communications have specific QoS requirements.

In most current 4G/LTE networks, the SMS service is based on IMS. Due to their demand for timeliness, SMS packets are usually sent in a dedicated bearer with QoS requirements that are higher than those of general IP packets. The IMS service utilizes the Session Initiation Protocol (SIP) [3] to handle SMS delivery. A SIP session is maintained between the phone's SMS application and the IMS server. In turn, the IMS server

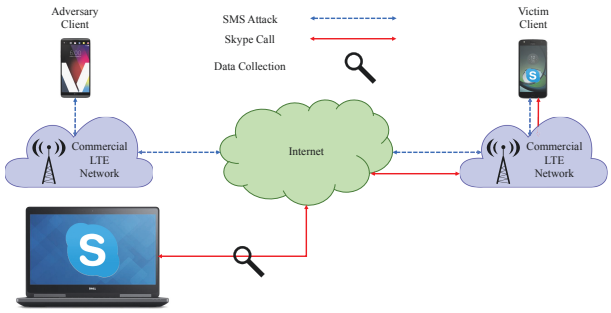


Fig. 2: Threat Model

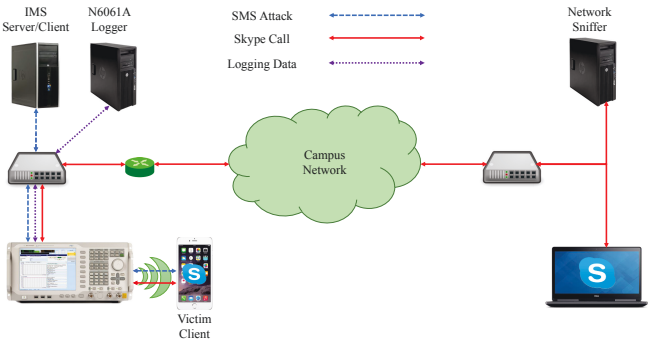


Fig. 3: A Local 4G/LTE Testbed

is responsible for bridging the SIP session and the SMS center.

III. Threat Model

We assume that the adversary's goal is to associate a target mobile phone number with a particular user account of a given IP-based service. Figure 2 illustrates the threat model. We assume that both the adversary's and victim's smartphones are connected to (likely different) commercial 4G/LTE networks. The attacker has the following capabilities:

1) The attacker can send SMS messages to the suspected phone number. We note that if the adversary can choose a message format incompatible with smartphones, for example CPIM [1], [4], the messages sent by the adversary will not be shown on the victim's phone. As a result, the victim is likely not aware of the adversary's messages.

2) The attacker can collect traffic generated by the application associated with the online account. We assume that the traffic is padded to a fixed packet size and then encrypted. The adversary has therefore no access to either content of the victim's communication or payload size.

3) The attacker is not free to pick the point where she observes the traffic. Obviously, the closer to the victim's phone the traffic is collected, the less interference the collected traffic data suffers from other traffic in the network. To illustrate the attack's effectiveness, we create a worst-case scenario, and we assume that the traffic is collected at the *furthest point* from the victim's smartphone, i.e., on the last hop of the traffic path.

4) We assume that the traffic collected by the adversary may be *aggregated*. There are many reasons (e.g., use of VPN) for why the adversary may not be able to filter the collected traffic to gain access to the traffic flow of interest. In other words, the collected traffic includes not only the traffic generated by the application of interest, but other traffic as well.

In the rest of this paper, we will be using Skype as an example for the IP-based service: The adversary suspects that a given Skype name is being used on a smartphone with a known phone number, and they will use a cross service attack to associate the Skype name with the number of the phone. Skype is a particularly attractive IP-based service for cross-service attacks: On one hand it is susceptible to timing-based side-channel attacks because of its need to provide quality-of-service. On the other hand, Skype prides itself to having a unique set of features to protect privacy of Skype calls, such as strong encryption and proprietary protocols [5], dynamic path selection [6], and constant packet rates [7].

IV. Account Association in A Local Testbed

In this section, we present our investigation of account association in a local testbed with 4G/LTE connectivity. We will use the term "identification" to denote the process of identifying if there is an association between a target phone number and a given user account. The approach to identify whether an association exists is therefore called an *identification approach*. At the end of this section we will present the performance of the described identification approach.

1) Local Testbed: Figure 3 illustrates the setup of the local testbed. The testbed is built around the Keysight LTE test solution, including an Agilent PXT E6621A LTE wireless communications test set, the E6966B IMS-SIP Network Emulator Software, and the N6061A LTE Protocol Logging and Analysis application. The victim's phone is connected to the PXT E6621A through 4G/LTE connections. The VoLTE service, including the SMS message service, is provided by the IMS server running the Keysight E6966B-1FP IMS-SIP Server Emulator Software. The adversary sends SMS text messages through the IMS client running Keysight. The Skype call comes in through a campus network, and the adversary observes Skype traffic from the victim's phone by collecting traffic on the farthest hop of the path of the Skype connection.

2) Identifying Account Association - Rationale: The identification of the account association is feasible because of the differences in the bearers (and their QoS levels in particular) used to transport Skype packets *vs.* SMS text messages. As described in Section II, SMS text messages are usually sent in a bearer with higher Quality of Service (QoS) requirements, typically same or similar to the QoS of bearers for VoLTE calls. This is because of SMS's close relationship to voice. General IP packets, including the Skype packets, are sent in the default bearer, which usually has lower QoS requirements [8]. This provides an opportunity to the adversary, who identifies the account association by sending SMS text messages to the victim's phone. Since the SMS messages are sent with higher QoS, the traffic of other IP services with lower QoS (Skype in our case) will be disturbed. The IP traffic will therefore display an inter-packet-time pattern that reflects the interference caused by the SMS messages. The adversary can

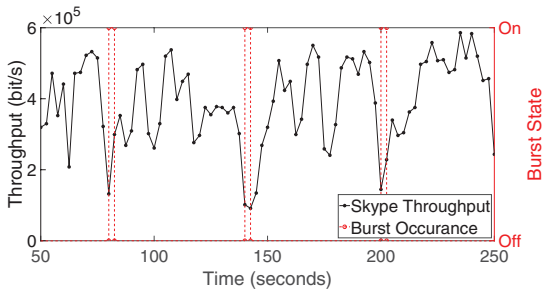


Fig. 4: Effect of SMS Messages on Skype Traffic

therefore identify the account association by correlating the timing of the SMS messages with the timing pattern of IP traffic (Skype in our case) generated by the victim's phone.

Figure 4 shows an example of the effect on Skype traffic caused by the interfering SMS messages. The graph shows the throughput of Skype traffic over time. In this example, three bursts of SMS messages are generated. We observe that each burst affects the rate of the Skype traffic. The results in this figure are obtained from the testbed shown in Figure 3. The length of the sampling window for the computation of the throughput curve is 2.5 seconds. These results illustrate the two primary challenges with identification: (1) The Skype traffic throughput fluctuates over time, and some decreases in the throughput curve may not be caused by the interfering bursts of SMS messages. (2) The size of bursts may be limited, and therefore may not be generating easily-detectable interference patterns. For illustrative purposes, the results in Figure 4 use a large number of SMS messages (425 messages) in each burst. Obviously, in real 4G/LTE networks it is not possible to send such large a number of SMS text messages in a burst because the network operators have limits in place on SMS message sending rates.

3) Identification Algorithm: To start the identification, the adversary sends a sequence of bursts with n SMS messages each. The adversary identifies the account association by detecting the pattern using Algorithm 1. The algorithm can be divided into three steps: data extraction, cross correlation, and decision. In the data extraction step, we first store the number of messages sent within each burst in the array b_{len}. We then store the number of packets collected during the corresponding time slots at the data collection point in array $traf$. We also randomly pick time slots that do not overlap with the burst periods. The number of messages sent during the randomly picked time slots is zero and kept in array b_{len} as well. Similarly, the number of packets collected during the corresponding time slots is kept in array $traf$. (We assume that we collect enough traffic at the collection point so that the arrays $traf$ and b_{len} are of the same size.)

We use the sample *Pearson's correlation coefficent* r to cross-correlate the values in arrays b_{len} and $traf$. SMS bursts can cause reductions in the rate of traffic sent from the victim's smartphone. If so, the two arrays will be negatively-correlated.

Based on the cross-correlation results obtained in the previous step, and collected in vector $corrval$, the function

input : n - number of SMS message bursts; len_{traf} - length of traffic collected at the data collection point; arrays b_{begin}, b_{end}, and b_{len} - with $b_{begin}[i]$, $b_{end}[i]$, and $b_{len}[i]$ indicating the start and end time of and the number of message in the ith burst, $blen_{avg}$ - average burst length, $bound$ - bound on the delay between the sending of a burst and the arrival of the corresponding pattern observed at the data collection point, δ - step increase;
output: dec - Detection decision ;
$\Delta \leftarrow 0$; $t \leftarrow b_{end}[1]$; $j \leftarrow 1$;
while $\Delta + b_{end}[n] < len_{traf}$ **do**
  for $i \leftarrow 1$ **to** n **do**
    $traf[i] \leftarrow$ the number of packet arrivals at the data collection point during $[b_{begin}[i] + \Delta, b_{end}[i] + \Delta]$;
    randomly pick one duration $[t_{random}, t_{random} + blen_{avg}]$ not overlapping with burst durations;
    $b_{len}[n+i] \leftarrow$ the number of SMS messages during $[t_{random}, t_{random} + blen_{avg}]$;
    $traf[n+i] \leftarrow$ the number of packets during $[t_{random} + \Delta, t_{random} + blen_{avg} + \Delta]$;
  end
  $corrval[j] \leftarrow r(b_{len}[1..2n],\ traf[1..2n])$;
  $j \leftarrow j + 1$;
  $\Delta \leftarrow \Delta + \delta$;
end
$dec \leftarrow$ `Decision`$(corrval)$;

Algorithm 1: Identification Algorithm for a Local Testbed

$Decision$ tells us whether the pattern is detected. Our experiments show that the cross-correlation values are close to Gaussian. We also observed that the cross-correlation values are very far away from the mean when the pattern is synchronized with the bursts. The decision logic is therefore simple: If within the bound of the delay between SMS message sending time and the arrival time of the corresponding pattern at the data collection point, the cross-correlation between the bursts and the traffic is less than the decision threshold (three standard deviations off the mean on the left side of the normal distribution,) the account association is confirmed. In our experiments, the $bound$ is roughly 1 second, as the SMS message delay is around 0.3987 seconds, and the packet delay between victim's phone and the data collection point is about 0.75 seconds. The $bound$ is much smaller than the length of bursts, which are about 1.5 seconds long.

4) Identification Performance: To evaluate the performance of the identification algorithm, we conducted experiments in the local testbed shown in Figure 3. In these experiments, SMS messages were sent in two different message formats: 3GPP2 [9] and CPIM [1], [4]. We choose the 3GPP2 message format because of its popularity. The CPIM message format was chosen because CPIM messages are received but can

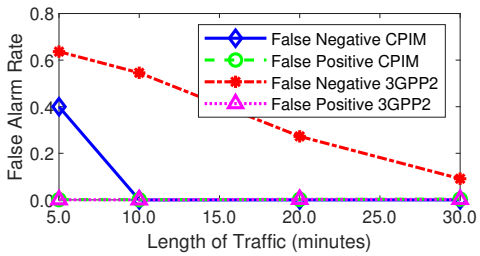


Fig. 5: Identification Performance in A Local 4G/LTE Testbed

not be displayed on smartphones such as the iPhone 6S Plus with iOS version 11.4 (15F79). We used the N6061A LTE protocol logging and analysis software in the testbed to verify that CPIM messages are indeed delivered to the iPhone by observing that the iPhone sends a confirmation of receipt. At the same time we observed that the iPhone shows no indication to the user that it received an SMS message. In other words, the victim receives no indication of the SMS message burst in the CPIM format because the messages will not be shown on the victim's phone at all.

Figure 5 compares the identification performance for SMS messages sent in the CPIM format and 3GPP2 format, respectively, for varying lengths of traffic observation. In both experiments, each burst contains 20 SMS messages, and the inter-burst time is on average two seconds. We observe that for messages sent in the CPIM format, both false-positive and false-negative rates are close to zero when the length of traffic is above or equal to 10 minutes. The false-positive rates for 3GPP2 are close to zero, and the false-negative rate drops to below 10% as the length of traffic observation grows to 30 minutes. From Figure 5, we also observe the differences in identification performance for the two message formats. We conjecture that the differences are caused by the handling of SMS messages sent in the CPIM format in iOS. It seems to us that the handling of SMS messages in the CPIM format is more resource-consuming, as the phone can not interpret the messages properly. This increases both the level of stealth and of effectiveness of the attack.

V. Identifying Account Association in a Major Mobile Network

The experiments in the local testbed show that the identification of account associations is possible in principle. In this section, we address the question of whether attacks of this type can be staged in a real-world commercial network as well. The following experiments were conducted on one of the four major U.S. mobile networks.

1) Experiment Setup: Figure 2 shows the experiment setup to replicate the previous local experiments over a major mobile network in the United States. In this setup, the adversary stages the attack by sending SMS bursts over a commercial 4G/LTE network, in this case using an LG V20 smartphone. The victim's phone is a Motorola Moto Z Play Droid running Skype version 8.36.0.52, and it is connected to a commercial 4G/LTE network as well.

2) Challenges: The mechanisms used by service operators to run messaging over commercial networks are expected to render the direct application of the attack as described in Section IV ineffective. Challenges arise primarily from the need to protect network resources with the help of scheduling and service throttling in two locations: (1) SMS *service centers* in mobile networks are responsible for storing, forwarding, and delivering SMS messages [10]. These centers are also responsible for maintaining the service operation, such as message delivery reports to message senders. Since SMS service centers are shared by many service subscribers, messages from different subscribers may get *queued*, and their processing may need to be *scheduled* by the service center. The networks also put limits on message sending rates [11], [12]. If subscribers exceed these limits, their message deliveries are *throttled* by the service center. (2) The *uplink* bandwidth is shared among 4G/LTE service subscribers, and scheduling is used for resource control [13]. This leads to queuing and delays.

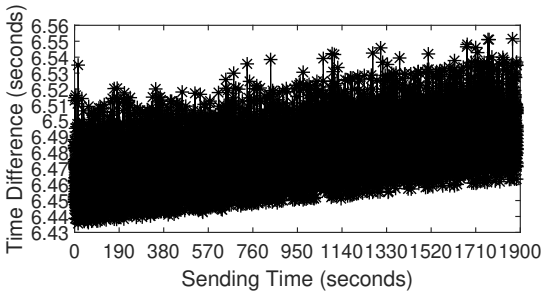
Figure 6 shows the delay between message sending time at the adversary's smartphone and corresponding message receiving time at the victim's smartphone. The delay in the commercial 4G/LTE network, as shown in Figure 6b, can vary from 0.2 seconds to about 350 seconds. Similar saw-tooth patterns of packet round-trip times have been observed in 4G/LTE networks before [13], and the saw-tooth pattern has been mainly attributed to the scheduling protocols. Similarly, the saw-tooth patterns in message delays observed in our experiments can be largely explained by the scheduling in mobile networks. In our experiments, the periodicity is much longer because the scheduling can also happen at the SMS message level. The delay in the local testbed, as show in Figure 6a, only varies from about 6.43 seconds to about 6.55 seconds. This is largely because only very few smartphones are connected to the local 4G/LTE network.

Figure 7 demonstrates the presence of throttling: Initially, the SMS messages are delivered in a burst of 20. As time progresses, the burst size is reduced by the service center, reaching a steady-state of 10 messages per burst.

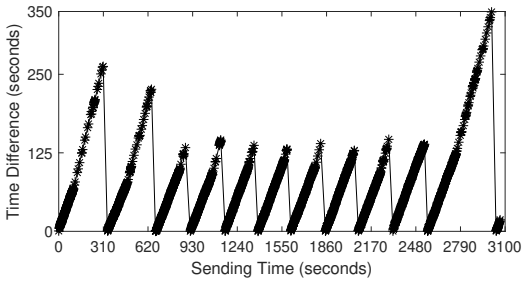
As a result of the scheduling and throttling, the identification algorithm presented in Section IV is ineffective in commercial 4G/LTE networks. The pattern caused by the SMS message bursts is not detectable in large networks because the scheduling and throttling of message delivery spread out bursts of SMS messages and make them difficult to detect.

3) Identification in a Major Mobile Network: Effective account association is still possible. We observe from Figures 6b and 7 that the burst-spreading effect due to scheduling and throttling is not immediately evident at the very beginning of SMS bursts. Instead, the spreading caused by scheduling and by throttling only gradually take effect over the length of one or more bursts. This effect is easily understandable, as any scheduler and any form of rate controller or throttling mechanisms must first detect the bursts before it can kick in and take action on the SMS messages.

Based on these observations, we re-design our identification algorithm to detect the *increase* of burst spreading, rather than



(a) Local 4G/LTE Testbed



(b) Commercial 4G/LTE Network

Fig. 6: Time Difference Between Sending and Receiving a Text Message

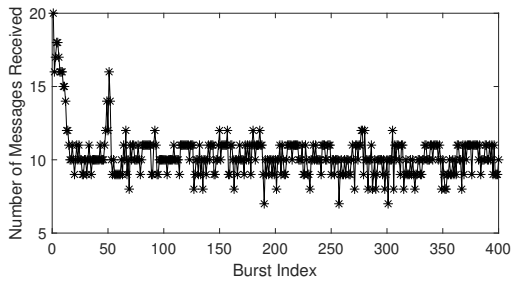


Fig. 7: Throttling in A Commercial 4G/LTE Network

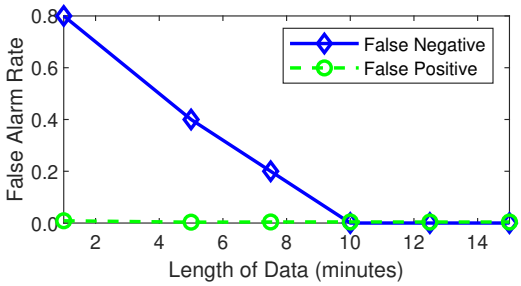


Fig. 8: Identification in Commercial 4G/LTE Network

the burst interference directly such as done in Algorithm 1. The major differences from Algorithm 1 are as follows: (1) The cross-correlation is between SMS bursts and delayed versions of traffic possibly containing patterns affected by the spreading and throttling. (2) The random sampling related to t_{random} is removed because the detection focuses on the spreading and throttling effects on SMS bursts only. (3) We fix the sample interval, i.e., the interval used to count the number of SMS messages ($b_{len}[i]$) and packets ($traf[i]$), to be the minimal length of all the bursts in time.

4) Identification Performance: Figure 8 shows the identification performance of the new algorithm for 20 messages per burst and two-second average time between message bursts. We observe that the false-positive rate is close to zero, false-negatives are about 20% when the traffic length is about 7.5 minutes long and drop to 0% when it is 10 minutes or longer.

VI. Discussion and Conclusion

In this paper we direct the attention to an emerging class of attacks that is enabled by the increase deployment of platforms that run a variety of different services in an integrated fashion. Such platforms enable attacks to leverage information on one service to attack, or at least infer information about, users on another service. We call these attacks "cross-service attacks". The goal of this attack is to associate a target mobile phone number with a user account of an IP-based service.

Unfortunately, the need to operate SMS at low latency to very large numbers of subscribers renders it very difficult for the operator to prevent many timing attacks, including the ones described in this paper. In our future work, we plan to investigate approaches to mitigate the attacks and in the mean time without significant degradation on QoS of VoLTE packets.

References

[1] G. Klyne and D. Atkins, "Common Presence and Instant Messaging (CPIM): Message Format," RFC 3862, Tech. Rep. 3862, Aug. 2004.

[2] E. Elkin. (2014) The Secret Value of VoLTE. [Online]. Available: http://blog.tmcnet.com/next-generation-communications/2014/04/the-secret-value-of-volte.html

[3] E. Schooler, *RFC3261: SIP: Session Initiation Protocol*, Jun 2002.

[4] Android developers: Smsmanager. [Online]. Available: https://developer.android.com/reference/android/telephony/SmsManager

[5] T. Berson, "SKYPE SECURITY EVALUATION," Anagram Laboratories, Tech. Rep. ALR-2005-031, October 2005.

[6] S. A. Baset and H. G. Schulzrinne, "An analysis of the skype peer-to-peer internet telephony protocol," Tech. Rep., 2004.

[7] A. Awan and R. Venkatesan, "Design and implementation of enhanced crossbar CIOQ switch architecture," in *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*, vol. 2, May 2004, pp. 1045–1048 Vol.2.

[8] C. Gessner and O. Gerlach, "Voice and SMS in LTE," Rohde and Schwarz, White Paper 1e, May 2011.

[9] H. Garudadri, *RFC4393: MIME Type Registrations for 3GPP2 Multimedia Files*, Mar 2006.

[10] "Voice Over LTE: The New Mobile Voice," Alcatel-Lucent, Tech. Rep. m2012042721, April 2012.

[11] "AT&T Messaging Toolkit: Your Everything Mobile Communications," AT&T, Tech. Rep. AB-2241-01, May 2017.

[12] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks," in *Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 1118–1130.

[13] I. Hadžić, Y. Abe, and H. C. Woithe, "Edge Computing in the ePC: A Reality Check," in *Proc. of the Second ACM/IEEE Symp. on Edge Computing*, ser. SEC '17. New York, NY, USA: ACM, 2017, pp. 13:1–13:10.