A framework for anonymizing GSM calls over a smartphone VoIP network

Ioannis Psaroudakis, Vasilios Katos, and Pavlos S. Efraimidis

Information Security and Incident Response Unit
Department of Electrical and Computer Engineering
Democritus University of Thrace
University Campus, Xanthi 67100, Greece
{jpsaroud}@duth.gr
{vkatos,pefraimi}@ee.duth.gr
http://isir.ee.duth.gr/

Abstract. The proposed framework describes a service for users that gives them the ability to make gsm calls from their smartphones without revealing their identity. The principle to achieve that is simple: instead of using your cell phone to make a call, pick somebody else's phone to do so. We proposed an infrastructure of smartphones, sip registrars and sip proxies to provide caller anonymity. We developed a testbed where a smartphone registers on a SIP registrar and can start GSM conversation through another smartphone acting as a GSM gateway, by using a SIP proxy. Empirical evaluation revealed no significant QoS degradation.

Keywords: privacy; sip; smartphone; gsm anonymity

1 Introduction and motivation

Resource sharing in community networks is a well established concept since the dawn of the Internet. This has recently evolved through peer to peer networking, to grid computing and finally to cloud computing services, as the benefits of the collective paradigm are non disputable.

In the meantime, the wide adoption and commercial success of mobile networks due to the advances of wireless communications has resulted to the smart phone being the most preferred device for communicating through a variety of platforms. However a mobile phone device is not built with privacy in mind; the users location, preferences and behavior in general is recorded and shared between parties that offer the infrastructure, software, and operating system.

GSM calls are well regulated. Users are bound to a mobile number according to a regulatory framework and carriers are obliged to keep logs of their telephony conversations for a period of up to two years (Data Retention Directive 2006/24/EC).

In this paper we argue that certain privacy goals could be achieved by the active participation and collaboration of a community of users. We focus on VoIP and mobile communications and present a proof of concept for performing

telephone calls on a mobile network with caller anonymity. In the context of this paper, caller anonymity relates to the caller id and the call metadata; the underlying audio stream will be susceptible to passive eavsdropping by the callee's provider.

2 Related work

Requirements and specifications for offering caller anonymity over SIP are defined in RFC3323 [1] for three use cases relating to withholding the identity from the intermediary parties, the final destination(s), or both.

Quality of Service (QoS) is a critical factor that needs to be considered when designing and deploying any kind of telephony communication. A prevalent QoS feature for telephone communications is the delay [5], both while establishing a session and, most importantly, during the actual session for the voice stream. These parameters affect significantly the choice of the appropriate privacy enhancing technology. In [2] the authors present the main categories of PETs and conclude that a large number of technologies cannot be integrated with a VoIP solution like SIP due to their negative impact on the QoS attributes. For instance, Onion Routing [3] and Mixes [4] exhibit high call delays, whereas Hordes [9], DC-Nets and pMixes [7] may be more suitable but the latter has scalability issues as the underlying computational cost is in $O(n^2)$. In addition, many technologies were not designed or implemented with a view to be applied in VoIP communications (Onion Routing for example) and as such they do not inherently support UDP which makes them suitable only for the call initiation phases. The principle behind our proposed scheme is similar to that of crowds [8]. However the main difference is that in crowds anonymity is achieved by routing communication randomly within a group of similar users whereas in our proposition we do not allow direct communication between users and traffic is routed through special sip protocol capable entities.

3 The proposed scheme

The main idea behind the proposed scheme rests on the assumption that a participant (or smart phone owner) is voluntarily willing to offer her equipment for other users to make calls. This setting leads to two advantages. First, the carrier would not be able to establish the identity of the real caller. Second, there could be no charge at all if the offering person has an unlimited time contract with the carrier. Clearly the success of the proposed scheme relies on ease of use, reliability and level of participation in accordance to Metcalfe's Law [6].

The requirements and issues for a practical solution involve the discovery of users willing to offer their phones as SIP-GSM relays, the discovery of call destinations every user can offer and the protection of participants from malicious peers.

Throughout the scheme the following roles and entities are identified:

- *Caller*: This role refers to the main beneficiary of the infrastructure which is the user that wishes to make a call to a user (callee) with a selective preservation of her anonymity. Alice will be caller in our examples.
- *Callee*: The user that accepts a call. Bob will have this role.
- *SIP-to-GSM gateway*: The user that acts as a VoIP to GSM gateway and shares her GSM service. In our scheme, Carol will have this role.
- *SIP Registrar*: The registrars maintain the user SIP accounts and act as back-to-back user agents [11]. We assume the trusted entities Registrar A (for Alice) and Registrar C (for Carol).
- *SIP Proxy*: Proxies act as intermediaries on the communication path providing call routing. We assume a single SIP Proxy entity in one of the scenarios.
- *GSM Carrier*: This role offers the GSM mobile phone service. We assume the entities GSM carrier A, C and B, for Alice, Carol and Bob respectively. GSM Carrier A will is assumed to be malicious.

3.1 The anonymous communication scenario

Alice wants to communicate with Bob using her smartphone whilst maintaining her anonymity from Bobs carrier. More importantly, the GSM carrier of Alice should not learn anything about this phone call. Alice knows that a community of VoIP and GSM users is willing to help by sharing their phone and credits from their contracts. The easiest way is to communicate with some appropriate member (Carol) of the community by using the Internet infrastructure. Carol's device must be able to communicate with Alice using the Internet through her WIFI or HSPA connection and at the same time to call Bob using the GSM connection. This particular operation fulfilled by Carol is a so-called a SIP-to-GSM gateway operation and it is the kernel function for the service. The operation has to take place without any actions taken from Carol apart from her declaration of consent to lend her resources.

The user registration process should cover both roles the participants will have, that is Caller and SIP2GSM gateway. The users register to the SIP registrars and provide data such as user credentials, sharing resources, policy data and SLAs. SIP registrars are assumed to be trusted and to act as agents on behalf of the users. Every SIP Registrar in turn needs to be affiliated with at least one SIP proxy server. The affiliation is initiated with the SIP registrar administrator who will provide the data similar to the user registration process to the proxy server during the application process.

We define the following privacy requirements:

P1 *Caller anonymity in the GSM network.* Alice's identity should be hidden from GSM provider A.
P2 *Mutual anonymity between the caller and the gateway.* Alice should not know that her call is routed through Carol and vice versa.
P3 *SIP-to-GSM gateway privacy.* The gateway's personal information, including its contracts and capabilities should only be available to SIP Registrar C.

P4 *SIP Registrar privacy.* There will be no leakage of the information maintained by the SIP registrars A and C.

Although in principle the caller's anonymity in the GSM environment can be trivially offered due to the apparent "incompatibility" of the two networks, the caller's identity could be discovered from the actual voice stream which the GSM has access to. In general terms, this is considered as a probabilistic side channel, since the probability of identifying the caller from the available audio data is not necessarily equal to one. Furthermore, mutual anonymity is also required between the caller and the gateway. Anonymity of the caller is required because in the opposite case if Carol (the gateway) is malicious or a passive eavesdropper or (even worse) belongs to the GSM carrier, then she will have access to both the caller and the callee information. Therefore, P1 depends on P2.

P3 is perhaps the most important requirement. All information provided by the gateway needs to be protected as in the opposite case a curious participant may collect valuable data and generate statistics over the users and their contracts, which then can be used for personal gain. P3 also depends upon P4 which is offered by design.

3.2 Private VoIP to GSM gateway discovery

A fully developed version of our system will have to address additional privacy issues that arise in auxiliary functions of the system. An example is the gateway discovery procedure discussed earlier. If the SIP Registrar A is trusted (as we assumed earlier) then the privacy of Alice is preserved while requesting to use the platform for a call to Bob. Similarly, if the Registrar C of Carol is trusted then Carol can safely advertise her readiness to act as SIP-to-GSM gateway for specific GSM carriers. The above scheme can be futher improved by adding a SIP Proxy to it. However, in all these cases, privacy relies on assumptions about the participating entities and/or the introduction of a proxy. A challenging requirement would be to solve the same problem for Honest-but-Curious or even malicious entities, by applying advanced cryptographic techniques [12]. We are currently examining a similar service for the needs of our application.

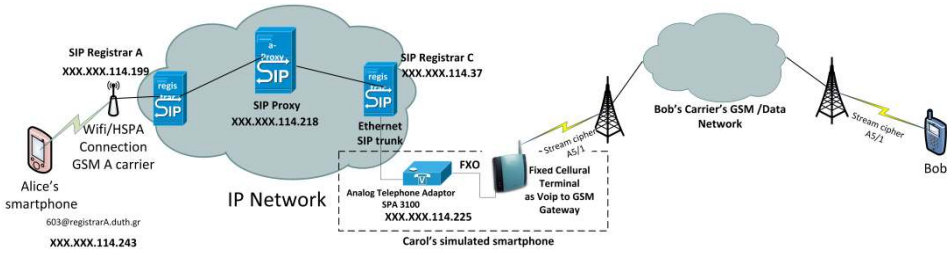

Fig. 1. The testbed environment

A framework for anonymizing GSM calls over a smartphone VoIP network 5

3.3 Performance evaluation

Telephony applications require real time audio streaming and are tightly coupled with QoS network parameters. We therefore need to investigate whether the proposed solution with the added security controls will not have negative impact on the user acceptance.

We proceed on implementing the proposed framework and making our first anonymous calls. We used two CentOS servers with Asterisk software as SIP registrar entities, a PC with TekSIP software as the Proxy server and a VoIP ATA (Linksys SPA3000) with Ericsson's FCT as VoIP-to-GSM gateway (Fig. 1) simulating the application to be developed for smartphones. The initial caller (Alice) was an android smartphone running CSipSimple. For the data collection and analysis we used a 2960G Gigabit Cisco switch with port monitoring enabled to gather the call flow that shows the SIP negotiation (Fig. 2).

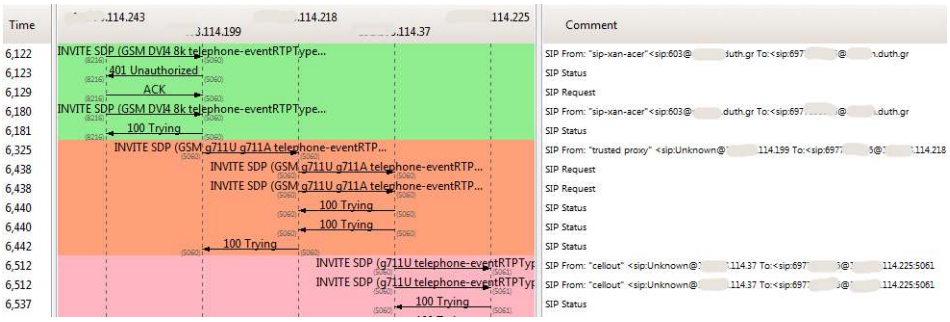

Fig. 2. Excerpt from the anonymised SIP flow using wireshark

From the call flow and the SIP methods it can be seen that Alice is unaware of the initial caller. None of the entities has full knowledge of the path of communication. As long as the proxy does not update the Via header in SIP INVITE as RFC 3261 [11] suggests, neither of SIP registrar has knowledge of each other:

```
INVITE sip:6977555555@x.x.114.37 SIP/2.0
Via: SIP/2.0/UDP x.x.114.218:5060;branch=z9hG4bK-2f6032f6;rport
Via: SIP/2.0/UDP x.x.114.199:5060;branch=z9hG4bK23f26f06;
```

Finally we performed a stress test with varying number of connections. It was established that the call on the SIP side, with one proxy (that is four SIP nodes in total) the majority of the calls can be established within a period of 500ms. This, compared to the GSM delay which is in the order of 8-12 seconds, is negligible.

4 Concluding remarks and areas for future research

We have described a framework for providing caller anonymity from their GSM by utilising a VoIP infrastructure and used SIP as a means to identify the is-

sues and explore possible design and implementation alternatives. Following our empirical investigation, we concluded that adding such an infrastructure on a GSM network will add negligible delays in the call establishment, as the bottleneck remains on the GSM side. Another area of research is in the development of a protocol so that each affiliated registrar advertises its network routing capabilities to the affiliated proxy in a dynamic way. As this proposed solution is defined over a novel configuration of a heterogeneous network, further security analysis of relevant threat vectors and corresponding countermeasures must be conducted. For example, a VoIP bot running on the proposed infrastructure could make excessive resource allocation and as such an anti spam over Internet Telephony mechanism must be deployed [10]. Lastly, legal issues must be looked into when offering such a service in public.

Acknowledgments This work was performed in the framework of and partially funded by the GSRT/CO-OPERATION/SPHINX Project (09SYN-72-419) (http://sphinx.vtrip.net)

References

1. Peterson, J.: A Privacy Mechanism for the Session Initiation Protocol (SIP). `http://cabernet.tools.ietf.org/html/rfc3323` (2002)
2. Kazatzopoulos, L., Delakouridis, C., Marias, G.F.: Providing anonymity services in SIP. In: 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (2008)
3. Reed, M G, Syverson, P F, Goldschlag, D M.:Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications. 16(4), 482–494 (1998)
4. Chaum, D. L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90 (1981)
5. Stier, M., Eick, E., Koerner, E.: A Practical Approach to SIP, QoS and AAA Integration. Integration The VLSI Journal (2006)
6. Metcalfe, R.: Metcalfe's Law. IEEE Spectrum, 17(40), 53 (1995)
7. Melchor, C. A., Deswarte, Y.: From DC-Nets to pMIXes: Multiple Variants for Anonymous Communications. In: Fifth IEEE International Symposium on Network Computing and Applications, IEEE Computer Society Washington, DC, USA pp.163–172 (2006)
8. Reiter, M., Rubin, A.: Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1(1), 66–92 (1998).
9. Levine, B. N., Shields, C.: Hordes: A multicast-based protocol for anonymity. Journal of Computer Security, 10(3), 213–240 (2002)
10. Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., Ehlert, S.: SPIDER: A platform for managing SIP-based Spam over Internet Telephony (SPIT). Journal of Computer Security 19(5): 835–867 (2011)
11. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC 3261, `http://tools.ietf.org/html/rfc3261` (2002)
12. Kim, J., Baek, J., Kim, K., Zhou, J.: A privacy-preserving secure service discovery protocol for ubiquitous computing environments. EuroPKI 2010, 45–60 (2011)