POSTER: The Shy Mayor: Private Badges in GeoSocial Networks

Bogdan Carbunar
Florida International University
Miami, FL
carbunar@cs.fiu.edu

Radu Sion
Stony Brook University
Stony Brook, NY
sion@cs.stonybrook.edu

Rahul Potharaju
Purdue University
West Lafayette, IN
rpothara@cs.purdue.edu

Moussa Ehsan
Stony Brook University
Stony Brook, NY
mehsan@cs.stonybrook.edu

***Abstract*—Location based social or *g*eosocial networks (GSNs) have recently emerged as a natural combination of location based services with online social networks: users register their location and activities, share it with friends and achieve special status (e.g., "mayorship" badges) based on aggregate location predicates. Boasting millions of users and tens of daily check-ins, such services pose significant privacy threats: user location information may be tracked and leaked to third parties. Conversely, a solution enabling location privacy may provide cheating capabilities to users wanting to claim special location status. In this paper we introduce new mechanisms that allow users to (inter)act privately in today's geosocial networks while simultaneously ensuring honest behaviors. Implementations show that the solutions are efficient: the provider can support thousands of check-ins and hundreds of status verifications per second.**

I. Introduction and Motivation

Location based services (LBS) offer information and entertainment services to mobile users, that rely on the geographical position of their mobile devices. A recently introduced but popular example, is the geosocial network (GSN) – social network centered on the geographical position of its users. Services such as Foursquare [1], SCVNGR [2] or Gowalla [3] allow users to register or "check-in" their location, share it with their friends, leave recommendations and collect prize "badges". Badges are acquired by checking-in at certain locations, following a required pattern simultaneously with other users, i.e. multiplayer games, or obtaining the highest number of check-ins during a time window ("mayor" badge).

Besides keeping track of their friends' location, the user incentives for participation include receiving promotional deals, coupons and personalized recommendations. For service providers the main source of revenue is targeted ads. Boasting millions of users [4] and tens of millions of location check-ins per day [5], GSNs can provide personalized, location dependent ads. As such, the price of participation for users is steep: compromised location privacy. Service providers learn the places visited by each user, the times and the sequence of visits as well as user preferences (e.g., places visited more often) [6], [7]. The implications are significant as service providers may use this information in ways that the users never intended when they signed-up (e.g., having their location information shared with third parties [8], [9]).

While compromised privacy may seem a sufficient reason to avoid the use of such services, here we argue this is not necessary. Instead, we propose a framework where users themselves store and manage their location information. The provider's (oblivious) participation serves solely the goal of ensuring user correctness. This enables users to privately and securely check in and acquire special location based status, e.g., in the form of badges. Badges are defined as aggregate predicates of locations. Solutions can then be devised to support a variety of such predicates, including (i) registering a pre-defined number of times at a location or set of locations, (ii) registering the most number of times (out of all the users) at a location and (iii) simultaneously registering with k other users at a location. Given the recent surge of location privacy scandals and the associated liabilities [10], we believe that implementing such solutions is also in the service provider's best interest.

To this end, the problem has two main facets. On one side, clients need strong privacy guarantees: The service provider should not learn user profile information, including (i) linking users to (location,time) pairs, (ii) linking users to any location, even if they achieve special status at that location and (iii) building user profiles – linking multiple locations where the same user has registered. On the other side, when awarding location-related badges the service provider needs assurances of client correctness. Otherwise, since special status often comes with financial and social perks, clients have incentives to report fake locations [11], copy and share special status tokens, or check-in more frequently than allowed.

In this work we first introduce SPOTR , a venue-oriented location verification protocol, that allows GSN providers to certify the locations claimed by users. SPOTR relies on single-use, 2 dimensional QR codes, displayed on devices inside participating venues. Each QR code encodes information that only the venue can generate and the GSN provider can verify.

We then propose three solutions for the private, aggregate location predicate problem. In $GeoBadge$, a user can privately prove k check-ins at one venue or a pre-defined set of venues, where k is a predefined parameter. $GeoM$ extends $GeoBadge$ with provably time-constrained check-ins as well as arbitrary values for k. Finally, $MPBadge$ extends $GeoBadge$ with support for simultaneous check-ins from co-located users.

To achieve this, the solutions deploy cryptographic techniques such as threshold secret sharing, blind signatures, quadratic residuosity constructs and zero-knowledge proofs.

Clients collect special, provider-issued tokens during check-ins, which they either aggregate to build generic, non-traceable badges, or use to build zero-knowledge proofs of ownership. Client correctness is partly ensured by the use of blind signatures of single-use tokens. The solutions also rely on the use of anonymizers. While existing network anonymizers such as Tor [12] may be used, our contributions also include a novel, provider stored, delay tolerant anonymizer, with computation provided by existing clients.

II. Evaluation

We have implemented SPOTR , $GeoBadge$ and $GeoM$ protocols. In this section we briefly evaluate their performance. We have implemented SPOTR on a Revision C4 of an OMAP 3530 DCCB72 720 MHz BeagleBoard [13] system (Figure 1) and a Google Nexus One smartphone featuring a 1 GHz Scorpion processor, Adreno 200 GPU and a Qualcomm QSD8250 Snapdragon chipset with 512 MB RAM. A QR code is generated on the BeagleBoard in 50ms and decoded on the Nexus One in 190ms, at a distance of 20cm.

$GeoBadge$ and $GeoM$ are implemented on the Nexus One smartphone, when running the server side on a 16 quadcore server featuring Intel(R) Xeon(R) CPU X7350 @ 2.93GHz and 128GB RAM.

Figure 2 shows the performance dependency of most compute-intensive functions of $GeoBadge$ on k, the number of check-ins required, when the key size is set to 1024 bits. The client $StatVerif$ takes up to 21s when $k = 100$. However, the provider components are much faster: the $StatVerif$ takes less than 27ms, allowing the provider to support more than 2400 such operations per second. The $CheckIn$ cost is even smaller, less than 10ms for k=100, allowing more than 6500 simultaneous check-ins.

Figure 3 shows that the $StatVerif$ server side exhibits small linear increases with k, but is only 124ms when $k = m = 60$. The server can support thus 512 simultaneous $StatVerif$ runs per second. The client side is less then 4.6s even for 60 check-ins.

III. Conclusions

In this paper we study privacy issues related to aggregate location predicates in GSNs. We propose solutions that privately and securely build a variety of aggregate location predicates.

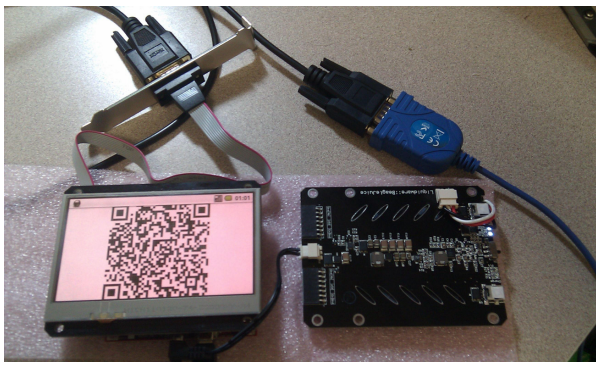

Fig. 1. Prototype of QR code based SPOTR on Beagleboard.

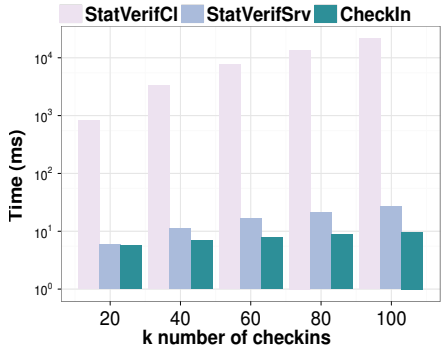

Fig. 2. GeoBadge dependence on k, the check-in count.

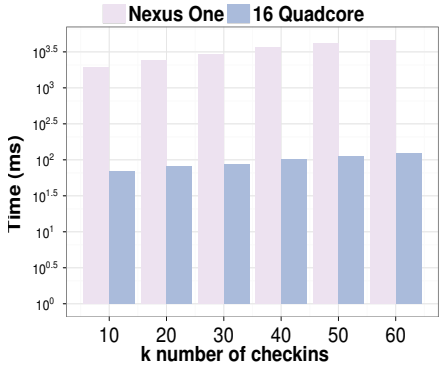

Fig. 3. $GeoM$: StatVerif client and server side, function of k, the number of check-ins

Our experiments show that the GSN provider can support thousands of operations per second, while a smartphone can build strongly secure aggregate location and correctness proofs in just a few seconds.

References

[1] Foursquare. https://foursquare.com/.

[2] SCVNGR. http://www.scvngr.com/.

[3] Gowalla. http://gowalla.com/.

[4] Lauren Indvik. Foursquare Surpasses 3 Million User Registrations. http://mashable.com/2010/08/29/foursquare-3-million-users/.

[5] Jolie O'Dell. Foursquare Day Sets Record with 3M+ Checkins. http://mashable.com/2011/04/20/foursquare-day-2/.

[6] Chloe Albanesius. Apple location, privacy issue prompts house inquiry. PC Mag. http://www.pcmag.com/article2/0,2817,2365619,00.asp.

[7] Jennifer Valentino-Devries. Google defends way it gets phone data. Wall Street Journal. http://online.wsj.com/article/SB10001424052748703387904576279451001593760.html, 2011.

[8] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. In *WOSN*, pages 7–12, 2009.

[9] Balachander Krishnamurthy and Craig E. Wills. On the leakage of personally identifiable information via online social networks. *Computer Communication Review*, 40(1):112–117, 2010.

[10] Josh Lowensohn. Apple sued over location tracking in iOS. Cnet News. http://news.cnet.com/8301-27076_3-20057245-248.html/, 2011.

[11] Gpscheat! http://www.gpscheat.com/.

[12] Roger Dingledine, Nick Mathewson, and Paul F. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320, 2004.

[13] G. Coley. Beagleboard system reference manual. *BeagleBoard. org, December*, 2009.