A Survey of Privacy Vulnerabilities and Defenses in GeoSocial Networks

Bogdan Carbunar, Mahmudur Rahman, and Niki Pissinou, Florida International University

Athanasios V. Vasilakos, National Technical University of Athens

The work of Bogdan Carbunar and Mahmudur Rahman has been supported by the Department of Defense under grant W911NF-13-1-0142.

ABSTRACT

Geosocial networks (GSNs) are a popular extension of the growing online social networking phenomenon. The wealth of personal information voluntarily revealed by subscribers, however, exposes them to a wide range of privacy vulnerabilities. In this article we describe basic GSN features and show how external attackers can exploit them in order to gain access to sensitive user information. We introduce several properties that need to be satisfied by a viable, privacy preserving GSN solution. We survey the body of work addressing GSN attacks and privacy issues, and compare their ability to satisfy the crystallized properties. Finally, we propose several open research directions.

INTRODUCTION

Online social networks are virtual connectivity hubs, allowing users to maintain contact with relations through the innovative "friend" concept: two users become friends if an invitation sent by one is accepted by the other. Geosocial networks (GSNs) are a recent but increasingly popular addition to this space. Sites like Foursquare, Yelp, and Google Latitude have garnered tens of millions of registered user accounts and receive tens of millions of unique user visits per month. GSNs center their functionality on locations, in particular the relation between users and registered businesses, also called venues. Users can report or "check in" their location at a venue, share this information with their friends, leave recommendations, and collect prize "badges."

GSN users are encouraged to reveal a wealth of personal information, including locations visited, friends, interests, and preferences. This information purportedly allows GSN providers to offer a variety of applications, and venue owners to promote their business through spatio-temporal incentives (e.g., rewarding frequent customers through accumulated badges). However, the profitability of providers and participating businesses rests on their ability to collect and capitalize on detailed user information.

Access to user information raises significant privacy issues. In this article, we focus on vulnerabilities generated by the knowledge of GSN location information. Learning a user's locations of interest, as well as patterns (e.g., locations visited more frequently, visit order, and dependencies) can be used for profiling purposes and to infer sensitive information. For example, Krumm [1] showed that two weeks' worth of driving GPS location traces of users can be used to deduce the coordinates of the homes of more than 5 percent of participants, with a median error below 60 m. Pontes *et al.* [2] proved that public location information available in Foursquare can be used to infer the home city of around 78 percent of analyzed users within 50 km (out of approximately 13 million users). Golle and Partridge [3] showed that the threat of re-identification for location data is much greater when the individual's home and work locations can both be deduced from the data: revealing where one lives and works at the granularity of census blocks is uniquely identifying for a majority of the U.S. working population.

Furthermore, Kostakos *et al.* [4] showed that users who are central to their social network are likely to reveal more of their location information; the friend who knows most of a user's locations is the one with the most common contacts and/or the greatest number of contacts. Thus, co-location events can be used to learn surprising additional user information. For instance, Crandall [5] showed that even a very small number of co-occurrences can be used to predict a friend relation with a high empirical likelihood.

Given precedents of leaking and even selling [6] subscriber data, providers can be considered natural privacy adversaries. Moreover, external attackers can rely on GSN vulnerabilities to also gain access to sensitive user information. GSN vulnerabilities stem mainly from the simplified social networking procedures (opening an account, sending and accepting friend invitations) and the difficulty of verifying the correctness of statements made by remote users.

Considering both GSN providers and external entities as possible attackers, this article describes a suite of attacks that enable external adversaries to achieve an almost equal footing with GSN providers concerning privacy breaching capabilities. Furthermore, we crystallize several requirements for private GSN solutions, and

0163-6804/13/$25.00 © 2013 IEEE

then investigate the ability of existing solutions to satisfy them. Finally, we discuss several open problems and propose future research directions.

System Model

A GSN ecosystem consists of a provider and supported users and venues (businesses with a location). The provider plays a central part: both users and venues have accounts that are stored and managed by the provider. In the following we summarize the basic concepts and functionality of the system.

User account creation: Users subscribe to a GSN provider by creating an account. Most online services have a minimal set of user account creation requirements: the user needs to provide only a name and an email address. The sole verification mechanism relies on the confirmation of the email address. The user is emailed information that needs to be retrieved to validate the user account.

Friend relations: GSNs inherit the friend relations of online social networks, where user A can send a friend invitation to another user, B. User B can accept, reject, or ignore the invitation. If B accepts the invitation, A and B become friends.

Check-ins: Subscribers are assumed to have mobile devices equipped with a GPS receiver (present on most smartphones). Users report their location through *check-ins* at venues of interest. During a check-in, the user device captures the GPS address and reports it to the provider. The provider returns a list of venues in the vicinity, and the user needs to select one.

Badges: Users can share their location with friends, and are awarded points and "badges" (e.g., "Adventurer," "Explorer," "Superstar," etc.) by providers. Venues including Ann Taylor, GAP, Starbucks, and Burger King have partnered with various GSNs to reward their frequent customers with substantial discounts.

Friend co-location notifications: Sites like Google Latitude allow users to share location information with friends in real time. Given proper permissions, the application notifies the user's friends when the user is in their vicinity.

Venue reviews: A factor differentiating GSNs from classic social networks is that they host accounts not only for users but also for businesses or events with associated locations (called venues), such as restaurants, shops, offices, and concerts. Users are encouraged to leave feedback for venues in the form of written reviews. Reviews include a numerical component, called *rating* (e.g., ranging from 1 to 5). An *average rating* value is provided for each venue, computed over all the ratings of its posted reviews.

Default permissions: Several social networks are plagued by privacy problems stemming from the default sharing of all account information of users with all other social network users. For instance, Gross and Acquisti [7] showed that only a minimal percentage of users in a college social networking site changed these default privacy preferences. The default privacy settings of Facebook are set to "public." Yelp user accounts are globally accessible.

Adversarial Model

We focus on two adversary models. First, we consider an adversarial GSN provider, who uses collected user data to extract additional potentially sensitive information. We assume this provider is honest but curious: it tries to learn more about users; however, it follows the protocols correctly. Second, we consider an external adversary capable of controlling multiple user accounts. This adversary is purely malicious, capable of using any combination of data capture, modification, injection, and replay attacks in order to harm the system. The external adversary can target not only users, but also the provider.

GSN Attacks

In this section we show how the GSN features introduced earlier can be exploited to bring external adversaries on an equal footing with the GSN provider. Specifically, the attacks enable adversaries to collect large amounts of GSN user information. We begin with a description of basic attack vectors, and then describe their use to collect user data on a large scale.

Attack Vectors

Sybil Attacks — We show that the validation of the user account creation procedure of most GSNs relies only on the verification of the user provided email address. Short-lived email addresses can be easily obtained for free (e.g., 10 Minute Mail[1]). This allows attackers to create multiple identities, also called *Sybils*.

Detecting social network Sybil accounts is a hard problem. Sybils are not bound to establish tight-knit communities among themselves, but can establish arbitrary connections to real accounts through the infiltration attacks described next. Furthermore, the penalty against this behavior is minimal: if a Sybil account is deactivated, the attacker can easily create a new one.

Bringing Sybils to Life — As shown by Wang *et al.* [8], Sybil accounts can be identified as having significantly different behaviors from regular accounts. To address this, adversaries can attempt to maintain active Sybil accounts that emulate real user behaviors. In order for this process to be scalable, adversaries need tools to automatically perform fraudulent activities. We describe here two techniques for automatically creating and reporting incorrect information to GSN providers: location cheating and posting fraudulent reviews.

To report incorrect locations through check-ins, Sybil account owners can use specialized applications developed for the most popular mobile ecosystems, such as LocationSpoofer[2] for iPhone and GPSCheat[3] for Android. He *et al.* [9] proved the feasibility of fake check-ins in Foursquare, where the client application obtains the GPS location data from the phone's GPS application programming interfaces (APIs). Attackers can also use variations of automatic text generators (e.g., SCIGen[4]) or hire crowdsourcing (e.g., Amazon Mechanical Turk[5]) work-

A GSN ecosystem consists of a provider and supported users and venues (businesses with a location). The provider plays a central part: both users and venues have accounts that are stored and managed by the provider.

[1] *10 Minute Mail: http://10minutemail.com.*

[2] *LocationSpoofer: http://goo.gl/59HMk.*

[3] *GPSCheat: http://www.gpscheat.com/.*

ers to effortlessly post fraudulent reviews from Sybil accounts. Crowdsourcing sites have been shown (e.g., Ott *et al.* [10]) to be efficient in recruiting fake review writers.

Third Party Data Collection

External attackers can attempt to collect publicly available user and venue account information. While GSN providers have access to finer-grained information (e.g., exact times of user actions, event dependencies), in the following we describe two attacks that enable external adversaries to collect significant amounts of sensitive user information.

Large-Scale Crawls — Attackers can crawl the accounts of GSN users and venues, effectively collecting all their public information. This attack applies to accounts that do not change the permissive default settings. While sites like Yelp restrict the frequency and number of HTTP requests from a single (IP address, account) pair, such defenses can be thwarted by attackers controlling multiple Sybil accounts.

Infiltration Attacks — Attackers controlling Sybil accounts can launch *infiltration attacks* in order to befriend unsuspecting users. The attacker sends an invitation from a Sybil account to an intended victim. If the victim accepts the invitation, her personal account information is implicitly shared with the inviter . The use of Sybil accounts is of central importance: besides preserving the attacker's anonymity, their use in parallel infiltrations allows the attacker to bypass social network limitations on the number of outstanding invitations (sent but not accepted) and the total number of friends an account can have.

The use of Sybil accounts is of central importance: besides preserving the attacker's anonymity, their use in parallel infiltrations allows the attacker to bypass social network limitations on the number of outstanding invitations (sent but not accepted) and the total number of friends an account can have.

Infiltration attacks are effective. Boshmaf *et al.* [11] showed that a surprisingly high percentage of invited social networking users accept invitations from strangers. While infiltration attacks apply to general online social networks, they are particularly effective in GSNs, where friends are closer in concept to Twitter's "follower" concept.

Design Guidelines

We identify a list of requirements that need to be satisfied by a privacy preserving GSN solution. In addition to user privacy, several other properties are vital to ensure the viability of solutions. GSN providers need to be convinced that embracing privacy will not impact their profitability:

- **Privacy:** Protect user account information from unauthorized access by the provider, users, and crawlers.
- **Functionality:** Preserve the functionality of applications currently provided by the GSN system.
- **Statistics collection:** Enable providers and participating venues to collect statistics over the data of visitors.
- **Investment:** Minimize the additional investment imposed on providers and venues.
- **Usability:** Minimize the necessary user involvement.

These requirements can be conflicting, making their simultaneous satisfaction a significant challenge. For instance, user privacy can be achieved by preventing GSN providers and venue owners from accessing any user information. However, indiscriminate denial of access to user information discourages participation and may hinder the ability to satisfy the functionality and statistics collection requirements.

Moreover, a classic approach for providing location privacy relies on spatial and temporal cloaking, where noise is introduced in the reported location and time values. While this approach may preserve the ability of providers to collect relevant statistics over visitor populations, it also trades accuracy for privacy: a significant amount of noise will affect the functionality of existing applications (e.g., friend co-location notifications), while insufficient noise may render the approach vulnerable to attacks (e.g., the home/work identification attacks of [1–3], described in the introduction).

Existing Solutions

We now survey the body of work addressing privacy challenges in GSNs. A first step in protecting the data of GSN users from access by external adversaries is through addressing the attack vectors of an earlier section.

Thwarting Data Collection Attacks

Sybil Account Detection — Wang *et al.* [8] proposed an innovative server side approach for detecting Sybils, based on the observation that Sybils have different click stream behaviors (traces of click-through events in a browsing session) than regular users. They define a distance between click stream sequences and use it to cluster user click streams.

Instead of detecting and removing Sybils, Yu *et al.* [12] proposed DSybil, a defense tool for reducing their impact on recommendation systems (e.g., Digg's news recommendations). DSybil exploits the heavy-tail distribution of the typical voting behavior of the honest identities, and determines (for each news item) whether the system needs more feedback or has had "enough." Molavi *et al.* [13] adopt a similar approach to limit the impact of ratings bought or provided from Sybil accounts. They associate weights with ratings and introduce the concept of "relative ratings": a user's rating is transformed to a ranking relative to all the ratings given by the user.

Prevent Fraudulent Check-Ins — Carbunar and Potharaju [14] have introduced several location verification mechanisms that rely on the participation of concerned venues. A venue needs to install a device equipped with local communication capabilities (e.g., WiFi, near field communication [NFC]). During a check-in, the user device needs to establish a local communication channel with the venue device and run a location verification protocol. The weakness of the solutions, however, rests in their reliance on venue investments and their ability to manage additional equipment and applications.

[4] *SCIGen: http://pdos.csail.mit.edu/scigen/.*

[5] *Amazon Mechanical Turk: http://www.mturk.com.*

Detect Fraudulent Reviews — Ott *et al.* [10] were the first to propose techniques for detecting fraudulent GSN (TripAdvisor) reviews by focusing on the text of reviews. They have created the first database of fake hotel reviews from TripAdvisor. They integrated work from psychology and computational linguistics to develop and compare approaches to detecting deceptive opinion spam, including identifying several lexico-syntactic patterns indicating fake reviews.

While this approach is vulnerable to attackers learning and avoiding the identified patterns, Feng *et al.* [15] explore several alternative strategies, including one that relies on the hypothesis of a natural distribution of opinions in reviews. An attacker who hires people to write fake reviews will distort the distribution of review scores of the target venue, thus becoming detectable. The attacker may attempt to evade detection by modifying the representative distributions of review rating scores for the domain of the target venue. However, such an attack requires significantly higher investment on behalf of the attacker: hiring people to write fake reviews for multiple venues besides the intended target.

Existing approaches may be vulnerable to *framing* attacks: in order to discredit a competing venue, the attacker recruits workers to write fake reviews for that venue. This distorts the venue's distribution of review scores and raises questions about the venue's honesty.

Prevent Large-Scale Crawls — Mondal *et al.* [16] proposed Genie, a system that defends against large-scale crawls through credit networks built on the social network graph. Credit is associated with friend links, and each HTTP request consumes the credit on the links connecting the requesting account to the target account. This approach may prevent legitimate users from querying the social graph due to credit exhaustion. Furthermore, a GSN crawler is not required to be logged into a user account: sites like Yelp allow even non-subscribers to query user and venue pages.

Privacy Centric Solutions

In the following, we survey work that has focused on a variety of privacy issues in GSNs.

Puttaswamy and Zhao [17] argue that untrusted providers should be allowed to store only encrypted data, and move the application functionality to client devices. Users store "friendship" and "transaction" proofs on the provider site, cryptographically encrypted tokens encoding friend relations and messages, including location-centric reviews. The proofs can be accessed by any user, but can only be decrypted by those who know the decryption keys. Transaction proofs are stored in "buckets" associated with approximate locations (e.g., blocks), enabling users to retrieve information pertinent to their current location. This approach is thus able to support a wide variety of location-based applications, including collaborative content downloading, social recommendations, location-based reminders, or co-location events.

Mascetti *et al.* [18] propose solutions that hide user location information from the provider and enable users to control the information leaked to participating friends, with a view to improving service precision, computation, and communication costs. While they also employ user defined location privacy preferences, they use a combination of cryptographic constructs, including encryption, hashing, and secure computations, to allow users to privately determine co-location with friends.

Wernke *et al.* [19] propose the use of secret sharing and multiple non-colluding service providers to devise secure solutions for the management of private user locations when none of the providers can be fully trusted. The position of a user is split into shares, and each server stores one. A compromised server can only reveal erroneous user positions; the more servers are compromised (or maliciously collude), the higher their accuracy in reconstructing user positions. However, *all* servers need to be compromised in order to reveal exact user locations. We note that preserving standard GSN functionality is not a concern here. Furthermore, the feasibility of the approach rests on the ability to find multiple independent and altruistically managed servers.

Freni *et al.* [20] argue that the inherent nature of GSNs makes it hard for users to gauge their privacy leaks: GSN published content (e.g., photos with embedded GPS locations) is often associated with references to multiple users, making it difficult to determine which information is available and to whom it is available. Then, besides the location privacy problem, Freni *et al.* [20] also study the absence privacy problem — learning information about the absence of a person from a location at a specific time. The proposed solution requires users to specify their privacy preferences (e.g., in terms of the areas where their privacy should be preserved). The solution relies on a trusted third party (TTP) that processes posted locations according to user preferences before publishing them on the GSN provider. An advantage of the proposed solution is that it preserves the functionality of several GSN applications. Of further interest remains the investigation of the user ability to formulate and implement privacy preferences.

Luo and Hengartner [21] proposed VeriPlace, a secure, privacy preserving location validation framework. VeriPlace hides the location of users involved in the protocol, prevents malicious users from cheating (including wormhole attacks), and, by enabling the creation of location proofs with multiple granularity levels, maintains the functionality of applications that require various degrees of accuracy. VeriPlace achieves this through a two-step process. In a first step, it relies on access points (APs) to issue intermediate location proofs for users in their vicinity. In a second step, a trusted third party server converts intermediate proofs into final location proofs. VeriPlace provides this functionality through the use of ingenious cryptographic tools, including hash chains for building nested location proofs. Participating APs need to altruistically install and maintain additional software. Besides access points, VeriPlace requires the participation of three types of trusted third party servers. This effectively enables VeriPlace to

Existing approaches may be vulnerable to framing attacks: in order to discredit a competing venue, the attacker recruits workers to write fake reviews for that venue. This distorts the venue's distribution of review scores and raises questions about the venue's honesty.

Solution	Adversary type	Approach
Wernke *et al.* [19]	Provider	Multi-server
Freni *et al.* [20]	Provider+insider	TTP
Mascetti *et al.* [18]	Provider+insider	Crypto
Puttaswamy and Zhao [17]	Provider+insider	Crypto
Luo and Hengartner [21]	Provider	Multi-server TTP, crypto
Carbunar *et al.* [22]	Provider	Crypto

Table 1. *Comparison of adversary and approaches considered by private GSN solutions. TTP denotes trusted third party.*

detect collusion attacks involving users and defecting APs.

Carbunar *et al.* [22] made the observation that hiding user locations from providers and providing badges, an important GSN user participation incentive, are conflicting requirements. They proposed solutions combining cryptographic tools such as quadratic residues, secret sharing, and zero knowledge proofs to enable the private construction of badges. Upon performing a valid check-in, a user is privately issued a token by the provider. When enough tokens have been accumulated to warrant the creation of a badge, the user proves this fact to the server with zero knowledge (i.e., without revealing the owned tokens).

Table 1 shows the adversary model considered and the approach used by each surveyed solution. We note that solutions relying on cryptographic tools will incur a computation overhead. Care needs to be taken to ensure that the server overhead and client query latencies are minimized.

Table 2 summarizes the ability of solutions described in this subsection to satisfy the requirements introduced.

Open Questions and Directions

Thwarting GSN attacks: The challenges underlying GSN attacks have not been solved completely. For instance, the ease of creating fake accounts, emulating honest user behavior, and avoiding behaviors labeled as fake by existing research complicate the detection of Sybils, infiltration, and fake review attacks. Furthermore, existing location verification solutions need ground truth. Solutions that require venue investment and participation are expensive.

An approach that requires further investigation is to increase the work and cost imposed on attackers by fraudulent behaviors. For instance, the recommendation site Angie's List[6] requires paid membership. In addition to the financial cost, the use of personally identifiable information (i.e., per user credit card information) makes the creation of Sybil accounts a significantly complex process. Furthermore, fraudulent reviews can be eliminated by validating and verifying past user presence at reviewed venues.

Private statistics collection: The ability of current GSN privacy preserving solutions to privately build statistics over user populations is limited to counting the number of users visiting or checking in at a location. More complex statistics (e.g., determining the age and gender distributions of users or their visitor vs. local status) are essential in enabling venues to cater to their customers' needs and to improve the accuracy of personalized recommendations offered by providers. However, these statistics need to be computed privately (i.e., without learning individual participant information).

Private personalized recommendations: Current recommendation solutions either do not consider user locations or are not private. Providing private location-based recommendations is, however, an important requirement that has been overlooked by research so far. The problem is the following. Given the location history of a user (e.g., visited venues and their profile), enable the provider to *privately* identify:

- Similar venues (content-based filtering)
- Venues preferred by similar users (collaborative filtering)

Privacy here means that the provider does not learn the location history of the user, the user preferences, or the outcome of the recommendation process.

Solution	Privacy	Functionality	Investments	Stats collection	Usability
Wernke *et al.* [19]	✓	Range queries, proximity	High	X	✓
Freni *et al.* [20]	✓	Check-in, review, proximity	High	Visitor count	X
Mascetti *et al.* [18]	✓	Proximity	Low	X	✓
Puttaswamy and Zhao [17]	✓	Collaborative download, recommendations, proximity	Visitor count	Low	✓
Luo and Hengartner [21]	✓	Proximity, review, check-in	High	X	✓
Carbunar *et al.* [22]	✓	Check-in, badges	High	Visitor count	✓

Table 2. *Comparison of requirement satisfaction of various solutions.*

[6] *Angie's List: http://www.angieslist.com/.*

SUMMARY

In this article we have surveyed security and privacy vulnerabilities in geosocial networks as well as the current state of the art in defense techniques. We have discussed the features and opportunities provided by geosocial networks and have shown how they can be exploited by providers and external adversaries. Finally, we have identified open research questions and directions.

REFERENCES

[1] J. Krumm, "Inference Attacks on Location Tracks," *Pervasive*, 2007.

[2] T. Pontes *et al.*, "We Know Where You Live: Privacy Characterization of Foursquare Behavior," *Proc. 2012 ACM Conf. Ubiquitous Computing*, 2012, pp. 898–905.

[3] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," *Pervasive*, 2009.

[4] V. Kostakos *et al.*, "Who's Your Best Friend?: Targeted Privacy Attacks in Location-Sharing Social Networks," *Proc. 13th Int'l. Conf. Ubiquitous Computing*, 2011, pp. 177–86.

[5] D. J. Crandall *et al.*, "Inferring Social Ties from Geographic Coincidences," *Proc. Nat'l. Acad. Sci.*, vol. 107, no. 52, 2010, pp. 22,436–41.

[6] D. Reisinger, "Facebook Selling User Content to Advertisers," *CNET News*, http://news.cnet.com/8301-13506_3-20029593-17.html, Jan. 2011.

[7] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," *Proc. 2005 ACM Wksp. Privacy in the Electronic Society*, 2005.

[8] G. Wang *et al.*, "You are How You Click: Clickstream Analysis for Sybil Detection," *Proc. USENIX Security*, Washington, DC, Aug. 2013.

[9] W. He, X. Liu, and M. Ren, "Location Cheating: A Security Challenge to Location-based Social Network Services," *Proc. IEEE ICDCS*, 2011.

[10] M. Ott *et al.*, "Finding Deceptive Opinion Spam by Any Stretch of the Imagination," *Proc. 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, vol. 1, Stroudsburg, PA, Assn. Computational Linguistics, pp. 309–19.

[11] Y. Boshmaf *et al.*, "The Socialbot Network: When Bots Socialize for Fame and Money," *Proc. Annual Computer Security Applications Conf.*, 2011.

[12] H. Yu *et al.*, "Dsybil: Optimal Sybil-Resistance for Recommendation Systems," *Proc. 2009 30th IEEE Symp. Security and Privacy*, Washington, DC, 2009, pp. 283–98.

[13] A. Molavi Kakhki, C. Kliman-Silver, and A. Mislove, "Iolaus: Securing Online Content Rating Systems," *Proc. 22nd Int'l. World Wide Web Conf.*, Rio de Janeiro, Brazil, May 2013.

[14] B. Carbunar and R. Potharaju, "You Unlocked the Mt. Everest Badge on Foursquare! Countering Location Fraud in GeoSocial Networks," *Proc. 9th IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Systems*, 2012.

[15] S. Feng *et al.*, "Distributional Footprints of Deceptive Product Reviews," *Proc. 6th Int'l. Conf. Weblogs and Social Media*, 2012.

[16] M. Mondal *et al.*, "Defending Against Large-Scale Crawls in Online Social Networks," *Proc. 8th Int'l. Conf. Emerging Networking Experiments and Technologies*, 2012.

[17] K. P. N. Puttaswamy and B. Y. Zhao, "Preserving Privacy in Location-based Mobile Social Applications," *Proc. 11th Wksp. Mobile Computing Systems and Applications*, New York, NY, 2010, pp. 1–6.

[18] S. Mascetti *et al.*, "Privacy in Geo-Social Networks: Proximity Notification with Untrusted Service Providers and Curious Buddies," *VLDB Journal*, vol. 20, no. 4, Aug. 2011, pp. 541–66.

[19] M. Wernke, F. Drr, and K. Rothermel, "Pshare: Position Sharing for Location Privacy Based on Multi-Secret Sharing," *PerCom*, 2012, pp. 153–61.

[20] D. Freni *et al.*, "Preserving Location and Absence Privacy in Geo-Social Networks," *Proc. 19th ACM Int'l. Conf. Information and Knowledge Management*, New York, NY, 2010, pp. 309–18.

[21] W. Luo and U. Hengartner, "Veriplace: A Privacy-Aware Location Proof Architecture," *Proc. 18th SIGSPATIAL Int'l. Conf. Advances in Geographic Information Systems*, New York, NY, 2010, pp. 23–32.

[22] B. Carbunar *et al.*, "The Shy Mayor: Private Badges in Geosocial Networks," *Proc. 10th Int'l. Conf. Applied Cryptography and Network Security*, 2012, pp. 436–54.

BIOGRAPHIES

BOGDAN CARBUNAR (carbunar@cs.fiu.edu) is an assistant professor in the School of Computing and Information Sciences at Florida International University (FIU). Previously, he held various researcher positions within the Applied Research Center at Motorola. His research interests include distributed systems, security, and applied cryptography. He holds a Ph.D. in computer science from Purdue University.

MAHMUDUR RAHMAN (mrahm004@cs.fiu.edu) is a Ph.D. candidate in the School of Computing and Information Sciences at FIU, working under the supervision of Dr. Bogdan Carbunar. He received his M.S. degree in computer science from FIU in 2012 and his Bachelor's degree in computer science and engineering from Bangladesh University of Engineering and Technology. He spent three years in industry before joining FIU. His research interests are in security and privacy with applications in online and geosocial networks, wireless networks, distributed computing systems, and mobile applications. He is particularly interested in studying the trade-offs between privacy and usability that are achievable in OSNs, and strives to provide privacy-aware efficient and secure solutions in that context.

NIKI PISSINOU (pissinou@cs.fiu.edu) is a professor in the School of Computing and Information Sciences at FIU. She has published over 250 research papers in peer reviewed journals, conference proceedings, and books chapters on networking, telecommunications, distributed systems, mobile computing, security, and aspects of nontraditional data management. She has co-edited over four texts in the area of mobile and wireless networking and systems, and over 14 IEEE and ACM conference proceedings. Her research has been funded by NSF, DHS, NASA, DOT, DoD, state governments, and industry. She has served as the General and Technical Program Chair on a variety of ACM and IEEE conferences. She has served as an editor of many journals, including *IEEE Transactions on Data and Knowledge Engineering*. She has also been the founder of many professional forums, including the ACM GIS.

ATHANASIOS V. VASILAKOS (vasilako@ath.forthnet.gr) is currently a professor at the University of Western Macedonia, Greece, and a visiting professor at the National Technical University of Athens, Greece. He has served or is serving as an Editor for many technical journals, such as *IEEE TNSM*, *IEEE TSMC-Part B*, *IEEE TC*, *IEEE TITB*, *ACM TAAS*, and *IEEE JSAC* Special Issues in May 2009, and January and March 2011. He is Chairman of the Council of Computing of the European Alliances for Innovation.

The challenges underlying geosocial network security attacks have not been solved completely. For instance, the ease of creating fake accounts, of emulating honest user behavior and avoiding behaviors labeled as fake by existing research, complicate the detection of Sybils, infiltration and fake review attacks.