SPRINGL 2008 Workshop Report
ACM SIGSPATIAL Workshop on Security and Privacy in GIS and LBS

E. Bertino, M.L. Damiani, P. Capolsini, P. El Khoury, H.Martin

The first Workshop on Security and Privacy in GIS and LBS (SPRINGL 2008) was held on November 4th at Irvine (CA) in conjunction with the ACM GIS Conference. The goal of the SPRINGL workshop series is to provide a forum for researchers working in the area of geospatial data security and privacy. Both security and privacy are critical for geospatial applications because of the dramatic increase and dissemination of geospatial data in several application contexts including homeland security, environmental crises, and natural and industrial disasters. Furthermore, geospatial infrastructures are being leveraged by companies to provide a large variety of location-based services (LBS) able to tailor services to users. However, despite the increase of publicly accessible geospatial information only little attention is being paid to how to secure geospatial information systems (GIS) and LBS. Privacy is also of increasing concern given the sensitivity of personally-identifiable location information. This is despite major advancements that have been made in secure computing infrastructures and the secure and privacy-preserving management of traditional (relational) data in particular. The Workshop spanned across security and privacy aspects, as they relate to the management of geospatial data and to the development of emerging LBS. Eight papers were selected for presentation and inclusion in the Workshop proceedings. In addition, the program included one invited talk by Gabriel Ghinita and an inaugural paper for SPRINGL by Elisa Bertino, Michael Gertz, Bhavani Thuraisingham, and Maria L. Damiani.

Invited talk and inaugural paper. The invited talk by G. Ghinita focused on the trade-off between privacy and efficiency in privacy-preserving techniques in LBS. A taxonomy of privacy solutions was presented defined on the basis of the location transformation being used and the system architecture being adopted. The classification identifies three categories of techniques: (a) two-tier spatial transformations, (b) three-tier spatial transformations and (c) cryptographic transformations. Cryptographic transformations based on Private Information Retrieval offer the strongest privacy guarantees but may incur very significant processing overhead likely exceeding that of spatial transformation methods. The paper by Ghinita also identified several open research issues.

The SPRINGL inaugural paper was presented by E. Bertino. The paper offers a comprehensive overview of the security challenges in geospatial data management and outlines a framework to deal with those issues. That framework encompasses a broad range of functions supporting: the specification of the policies and reasoning techniques for fine-grained access control to geospatial objects at varying resolution; interoperability of security policies for geospatial data; trust management, authentication, and secure third-party publication of geospatial data.

Papers. The 8 contributed papers were grouped in 3 sessions: Access Control Model for GIS and Pervasive Environments; Location Privacy; Policies.

Access Control Model for GIS and Pervasive Environments. *P. Capolsini* presented an extension of the Digital Right Expression Language ODRL to accommodate licensing for geographic data created by OpenGIS Web Map Services. The context-aware QACBAC access control model was presented by *J. Bringel Filho*. Such a model grants and applies permissions to users according to both context information and context quality indicators. *M.L. Damiani* discussed open issues related to the development of architectures and models for location-based access control models, proposing a shift from location-aware towards movement-aware access control.

Location Privacy. *N. Poolsappasit* presented a model for the specification of location privacy policies in LBS. Such a model targets the specification of context-aware privacy policies, in particular policies which typically depend on space, time and user category. *Y. Saygin* addressed the problem of how to make a trajectory database k-anonymous. A novel generalization-based approach was proposed that applies to trajectories and sequences in general. A different perspective was offered by *D. Lin* who presents a technique for the protection of location privacy in location-based queries such as "find my closest friends" based on the use of multiple agents for location transformation.

Policies. *P. El Khoury* proposed the use of description logics to define inter-organizational mappings for roles within a RBAC framework. Although those policies and methods are not specifically targeted to the geospatial domain, they can likely be extended for use in a mobile context.

Comments and research directions. The workshop was characterized by a lively and intense discussion on research issues and important challenges; we report some of these below:
1) Security and privacy models: There was agreement among the workshop participants that we are witnessing to a radical change of data infrastructures with the emergence of pervasive and ambient computing. Information is accessed from various places using mobile devices and personal data that can be acquired by sensor networks. In such a new world, we have to address the problem of the specification of adapted and contextual security policies. The associated languages and models should be able to integrate various knowledge representations by using formal descriptions like description logics.
2) Security of positioning models: Because many techniques for security and privacy of geospatial data depend on underlying assumptions about user position, security assurance about such positions is a key requirement. Also confidence about the trustworthiness of contextual information has been identified as critical by the workshop participants.
3) Security of IT applications in the domains of Homeland security, environmental crises, and natural and industrial disasters: All workshop participants agreed that these data-intensive applications need to be more reliable than in conventional IT applications. Typically these applications are a highly sought target by attackers (e.g. hackers, terrorists...) and are prone to unpredictable situations. Many challenging issues need to be addressed in order to secure those applications, including: How to setup security solutions for minimizing risks and for adapting to detectable but unpredictable situations? How to configure the security settings to adapt to these situations when people are on site?
Solutions building on workflow management systems seem reasonable in order to exploit the business logic layer as an attempt to be able to deal with unpredictable situations. Within this business layer geo-information can be captured and analyzed for adapting security solutions at

runtime. Moreover, security patterns could be an interesting area to explore for providing security as services deployable at runtime based on some pre- and post- conditions.
4) User privacy in mobile applications: Different approaches try to enforce the right for privacy, but noticeably very few are trying to work towards increasing the level of trust between the peers in mobile applications. Additional work for increasing trust level is indeed a different angle in order to enrich the solution for this privacy problem.
5) Benchmarks and scenarios: An important issue that was pointed out by various workshop participants is the lack of public datasets (such for example, datasets of trajectories) that can be used by the research community to carry out experimental research. Scenarios were also identified as relevant to assess real requirements concerning security and privacy of geo-spatial data.

Conclusions. The workshop was concluded by a short discussion about the future editions of the workshop. All participants were very positive about the outcome of the first edition of SPRINGL and very much in favour of organizing it again in 2009.