

Internship Opportunity: Verifiable Security for Parking Enforcement

K. Bhargavan and Michael J. May

Municipalities have been increasingly automating the management of the services offered to their residents, including smart metering, automated billing, and online applications for the issuance and checking of vehicle registration and permits. Such applications are convenient for residents and municipal employees alike, but also raise security and privacy concerns about how the data is stored, accessed, and used. The goal of this internship is to implement client and servers processes for an online service which verifiably provides information to municipal employees for specific purposes but prevents unauthorized or improper accesses.

We choose the example application of municipal parking enforcement where a pay-by-mobile parking service is offered. Parking enforcement officers are provided with GPRS enabled smart phones to query the status of vehicles in real time. The smart phone application queries the municipal parking service which checks its local database. The response returned to the smart phone may be “registered as parking legally” or “not registered”.

This internship will involve the development Java server software and smartphone client software for communication. The server and client software will be verified using Java Modeling Language (JML) [BCC⁺05]. The ideal candidate would have an interest in security and web applications, knowledge of Java. Java Modeling Language can be learnt during the internship.

This work can be extended in several possible directions, perhaps as part of a Ph.D. thesis. Two example extensions are:

- It is common practice for municipalities to outsource the management of the GRPS gateway. The third party gateway manager receives the queries from the officers and queries the parking provider’s database via a secured network connection to get a response. The gateway manager may introduce caching to improve response time and may not be trustworthy. A more complete system would include implementation and verification of an architecture involving such an intermediary. A similar idea can be found in [MSGL06].
- Another extension is the creation and verification of a composition of web services to manage on-street parking rights in addition to parking payment. Municipalities maintain multiple databases related to vehicles and parking: stolen vehicles registry, handicapped vehicles registry, vehicles subject to collection action registry, etc. When a parking enforcement officer sees a vehicle suspected of parking illegally, she queries an aggregating service (via a smartphone application which contacts the service via GPRS) and is returned either an “everything ok” or a list of violation codes for a citation or other followup. Security and privacy policies control which databases may be queried, in which order, and in what circumstances.

The main task is the development of a verifiably secure web service composition for parking enforcement. Our strategy shall be based on the adaptation of the security and privacy policies into a secure multiparty sessions representation which can be verified using the refinement type checker F7 [BBF⁺08, BCD⁺09]. This will involve a combination of programming with cryptographic libraries in Java, security analysis and bug-hunting, and formal verification using dependent type systems. Most of these skills can be learnt during the internship.

Application Details

The internship will be based at INRIA in Paris. The intern will have the opportunity to interact with security researchers at INRIA and at the Microsoft Research-INRIA Joint Center, including Cédric Fournet, Bruno Blanchet, Graham Steel, Pierre-Yves Strub, and Alfredo Pironti.

The internship is funded under a long-running ERC-funded project, called CRYSP, whose aim is to develop provably secure web applications. We expect the research carried out during the internship will form the major part of a Masters-level thesis and lead to a conference publication. We also expect to fund several Ph.D. students over the next few years.

To apply, send an email describing your research interests, and including your CV and the names and email addresses of two referees, to karthikeyan DOT bhargavan AT inria DOT fr. The deadline for applications is January 5th 2012.

References

- [BBF⁺08] Jesper Bengtson, Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, and Sergio Mafeis. Refinement types for secure implementations. In *Computer Security Foundations (CSF '08) Symposium*, 2008.
- [BCC⁺05] Lilian Burdy, Yoonsik Cheon, David R. Cok, Michael D. Ernst, Joseph R. Kiniry, Gary T. Leavens, K. Rustan M. Leino, and Erik Poll. An overview of JML tools and applications. *International Journal on Software Tools for Technology Transfer (STTT)*, 7(3):212–232, 2005.
- [BCD⁺09] Karthikeyan Bhargavan, Ricardo Corin, Pierre-Malo Deniérou, Cédric Fournet, and James J. Leifer. Cryptographic protocol synthesis and verification for multiparty sessions. In *Computer Security Foundations (CSF '09) Symposium*, 2009.
- [MSG⁺L06] Michael J. May, Wook Shin, Carl A. Gunter, and Insup Lee. Securing the drop-box architecture for assisted living. In *4th ACM Workshop on Formal Methods in Security Engineering: From Specifications to Code*, Fairfax, VA, Nov 2006.