

Undergraduate research project: Information Flow Policy Specification and Assurance for Bluetooth

This document describes an undergraduate summer research project on specification and verification of behavioral properties of Java programs, specifically secure information flow policy in parts of the Bluetooth wireless networking stack.

The work will support ongoing research of David Naumann and Gary Leavens in our project entitled “Collaborative Research: Formal Methods for Behavioral Subclassing and Callbacks”, which is funded by the US National Science Foundation (NSF). The summer research is funded as an NSF Research Experience for Undergraduates (REU).

The overall goal of the project is to advance the theoretical foundations of specification, development, and verification techniques for object oriented software, focusing on the widely used specification language JML¹ for Java. An area of particular importance for formal specification and verification is secure information flow.

We are seeking an undergraduate student who will carry out a case study in which JML will be used to specify information flow policies for selected components of an open-source Bluetooth implementation,² using the self-composition technique [BDR04, TA05, Nau05]. The ESC/Java³ tool will be used to verify that code conforms to policy. The primary objectives are to (a) assess the effectiveness of the self-composition technique and the relevant features of JML, in a substantial case study, and thereby form new research problems and priorities; and (b) to train a student in the requisite background to continue research in this direction. The student will be co-supervised by Naumann and by Prof. Susanne Wetzel at Stevens Institute of Technology.

Background. The PI has been working with Prof. Susanne Wetzel for several years on application of language-based security techniques in wireless network applications. In particular, we are developing CodeBlue, a collaborative music performance application based on Bluetooth wireless networking [HCV⁺03]. This system has been developed mainly by undergraduate students over several years, together with Prof. Susanne Wetzel, a cryptographer whose research focuses on wireless network security. CodeBlue serves as a testbed in which we experiment with attacks and countermeasures [NW03]. Many of the attacks that have been found in practice do not exploit cryptographic weaknesses but rather flaws in software API design and implementation; for this reason we are investigating static program analysis.

Although the working system uses Bluetooth for the sensor network, our focus has been on the application software. Last summer, Wetzel and Naumann jointly supervised two undergraduates working on access control within the CodeBlue music processing software, supported by REU awards. The work on access control was directed towards resource consumption attacks [JWY03].

Project plans. In the proposed project, an undergraduate student will develop security specifications for components of an open-source implementation of the Bluetooth protocol stack.⁴ He or she will use the pair composition technique to formulate specifications in

¹<http://www.jmlspecs.org>

²<http://www.javablueetooth.org/>

³<http://www.sos.cs.ru.nl/research/escjava/main.html>

⁴<http://www.javablueetooth.org/>

JML, and use the ESC/Java2 tool⁵ to check conformance of the code with the specifications. Integrity and confidentiality of PINS and session keys will be the main focus of policy. Besides checking the existing code, bugs and trojans will be introduced to implement attacks from Wetzel's research and the Bluetooth security literature. Complementary specifications may be formulated using the type system and inference tool under development by Qi Sun, but the main focus will be on verifying selected components of the Bluetooth stack, especially those involving declassification of encrypted data.

Project management and deliverables. A final report will be required as well as weekly status reports. The report will also be presented to Gary Leavens, co-PI, at his next research visit. As in preceding years, a demo will be presented at the Stevens undergraduate summer research fair in September. Depending on the results we may write a paper on the case study.

Naumann and/or Wetzel will meet face to face with the student at least 2–3 hours every week and be in daily contact by email. Additional help will be provided by the students who have worked previously on the CodeBlue system. The student will be required to be on campus during the 35 hour work week. Meetings will take place in the Lab for Secure Systems, where the networking, sensor, and music synthesis equipment is stored. Faculty are working to find nearby space (in addition to the general CS student lab) for all undergraduate researchers to be in proximity to each other and to the grad student offices.

Experience tells us that frequent contact is important for the student's learning and productivity; one benefit of two faculty advisors is that we can maintain close contact even when one is away at a conference.

Selection process and criteria. As in past years, the position will be advertised on the CS undergraduate mailing list and our web pages. We will interview students individually to assess their programming skill and familiarity with Java and Linux. The student should have taken a networking course. Just as important is a demonstrated ability to carry out sustained and productive activity on their own initiative. For this reason we are likely to choose a student who has distinguished herself in one of our courses or in the SENSE team.⁶

References

- [BDR04] Gilles Barthe, Pedro R. D'Argenio, and Tamara Rezk. Secure information flow by self-composition. In *17th IEEE Computer Security Foundations Workshop (CSFW'04)*, 2004.
- [BN05] Anindya Banerjee and David A. Naumann. Stack-based access control for secure information flow. *Journal of Functional Programming*, 15(2):131–177, 2005. Special issue on Language Based Security.
- [BN06] Anindya Banerjee and David A. Naumann. A logical account of secure declassification (extended abstract). Submitted for publication., 2006.
- [HCV⁺03] Dennis Hromin, Michael Chladil, Natalie Vanatta, David Naumann, Susanne Wetzel, Farooq Anjum, and Ravi Jain. CodeBlue: a Bluetooth interactive dance club system. In *IEEE Globecom*, 2003.
- [JWY03] Markus Jakobsson, Susanne Wetzel, and Bulent Yener. Stealth attacks on ad-hoc wireless networks. In *IEEE Vehicular Technical Conference*, 2003.

⁵<http://www.sos.cs.ru.nl/research/escjava/main.html>

⁶Supervised by Wetzel with Naumann's assistance, the SENSE team is a group of undergraduates who aim to develop a series of security attack and defense contests. See <http://www.stevens.edu/sense/>.

- [MPHL04] P. Müller, A. Poetzsch-Heffter, and G. T. Leavens. Modular invariants for layered object structures. Technical Report 424, Department of Computer Science, ETH Zurich, 2004.
- [Nau05] David A. Naumann. From coupling relations to mated invariants for secure information flow and data abstraction. Submitted for publication, July 2005.
- [NB04] David A. Naumann and Mike Barnett. Towards imperative modules: Reasoning about invariants and sharing of mutable state (extended abstract). In *IEEE Logic in Computer Science*, 2004.
- [NW03] David A. Naumann and Susanne Wetzel. High assurance for interactive applications in ad hoc networks. In *First International Workshop on Wireless Security Technologies*, April 2003.
- [SBN04] Qi Sun, Anindya Banerjee, and David A. Naumann. Modular and constraint-based information flow inference for an object-oriented language. In *Static Analysis Symposium (SAS)*, 2004.
- [TA05] Tachio Terauchi and Alex Aiken. Secure information flow as a safety problem. In *12th International Static Analysis Symposium (SAS)*, 2005.