PhD project in Information Security: Language-Based Security

Olaf Owe and Toktam RamezaniFarkhani

Feb. 15, 2017

In the modern society, information security is becoming increasingly important. Information security can be addressed from different perspectives including the application level, the hardware level, and operating systems, as well as the user level considering various human aspects. In this project we will focus on language-based techniques such as information-flow. Programming languages and information flow can provide fine-grained control of security aspects such as confidentiality and integrity because they allow accurate and flexible security information analysis of program components [1,2]. This mainly addresses the application level, but the choice of language constructs may also influence the design and security aspects of an underlying virtual machine.

We aim at providing security policy enforcement as a built-in and intrinsic language concept in object-oriented and distributed systems. For example, in order to specify and enforce information-flow policies, the effectiveness of language-based techniques has been established. Moreover, these policies usually dictate that no execution of the program should lead to an information-flow from more sensitive to less sensitive information holders [3,4]. This kind of security vulnerabilities cannot in general be addressed at the hardware or operating system level.

In this PhD project we will investigate security policies for object-oriented and distributed systems, and build on earlier work in language-based security and type systems [5] to develop more advanced security analysis, considering both theoretical developments and tool-oriented development, and considering both static approaches and run-time approaches. The work will involve development, and redevelopment, of language mechanisms, formal semantics, and tool-based analysis. Thus, background in formal methods, type systems, or formal semantics, is seen as an advantage. The project may be focusing towards theoretical contributions or more practical contri-

butions, partially depending on the candidate's background and interests.

- [1.] D. E. Denning, P. J. Denning, Certification of programs for secure information flow, Communications of the ACM 20 (7) (1977) 504–513.
- [2.] N. Heintze, J. G. Riecke, The SLam calculus: programming with secrecy and integrity, in: In POPL'98: Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 1998, pp. 365–377.
- [3.] J. A. Goguen, J. Meseguer, Unwinding and inference control, in: IEEE Symposium on Security and Privacy, 1984, pp. 75–75.
- [4.] D. Hedin, A. Sabelfeld, A perspective on information-flow control. In: Software Safety and Security - Tools for Analysis and Verification, Vol. 33 of NATO Science for Peace and Security Series - D: Information and Communication Security, IOS Press, 2012, pp. 319–347.
- [5.] D. Volpano, G. Smith, C. Irvine, A sound type system for secure flow analysis, Journal of Computer Security.