Security Evaluation and Hardening of FOSS

R. Charpentier
DRDC Valcartier
Robert.Charpentier@drdc-rddc.gc.ca

Prof. M. Debbabi
Concordia University
Debbabi@encs.concordia.ca

Abstract

Recently, Free and Open Source Software (FOSS) emerged as an alternative to Commercial-Off-The-Shelf (COTS) software. Now FOSS are perceived as a viable long-term solution that deserves careful consideration because of its potential for significant cost savings, improved reliability, and support advantages over proprietary software. However, the secure integration of FOSS in IT infrastructures is very demanding and methodologies must be adapted to reliably compose large FOSS-based software systems. A novel approach based on Aspect-Oriented Programming (AOP) was designed and tested in order to automate the security hardening process through a 4-year R&D effort carried-out at Concordia University under the leadership of DRDC Valcartier, Bell Canada and the Natural Sciences and Engineering Research Council of Canada. This paper presents this practical framework with the underlying solid semantic foundations for the security evaluation and hardening of FOSS. It also demonstrates with real-life software packages (eight well-known FOSS) that real-life vulnerabilities can be mitigated by this efficient paradigm (31 rules and 21 recommendations of the CERT standard).

Short Bios:

1- Mr. Robert Charpentier completed his degree in engineering physics at "l'École Polytechnique de Montréal" in 1979. After working at CAE Electronics on flight simulators, he joined Defence Research Establishment Valcartier, where he specialized in infrared imagery and space-based surveillance. His current research domains are secure interoperability, software formal certification, and software security design.

2- Dr. Mourad Debbabi is a Full Professor and the Director of the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada. He holds the Concordia Research Chair Tier I in Information Systems Security. He is also the Vice-President of the National Cyber Forensics Training Alliance (NCFTA Canada). He is the founder and one of the leaders of the Computer Security Laboratory (CSL) at Concordia University. He is the Specification Lead of four Standard JAIN (Java Intelligent Networks) Java Specification Requests (JSRs) dedicated to the elaboration of standard specifications for presence and instant messaging. In the past, he served as Senior Scientist at the Panasonic Information and Network Technologies Laboratory, Princeton, New Jersey, USA; Associate Professor at the Computer Science Department of Laval University, Quebec, Canada; Senior Scientist at General Electric Research Center, New York, USA; Research Associate at the Computer Science Department of Stanford University, California, USA; and Permanent Researcher at the Bull Corporate Research Center, Paris, France. Dr. Debbabi holds Ph.D. and M.Sc. degrees in computer science from Paris-XI Orsay, University, France. He published more than 170 research papers in journals and conferences on computer security, cyber forensics, formal semantics, Java security and acceleration, cryptographic protocols, malicious code detection, programming languages, type theory and specification and verification of safety-critical systems. He supervised to successful completion 12 Ph.D. students and more than 40 Master students. He can be reached at debbabi@ciise.concordia.ca. His webpage is accessible at http://www.ciise.concordia.ca/~debbabi