Semi-Automated Detection of Sanitization, Authentication and Declassification Errors in UML State Charts

**M.Sc. thesis problem statement**

Goal of the master thesis is to develop three source code checkers used for the detection of sanitization, authentication and declassification-function errors. Based on the open source Yakindu SCT framework the student will remodel 3 test programs (programs will be given) ((a) sanitization (CWE-78: Improper Neutralization of Special Elements used in a Command 'Command Injection') (b) authentication (CWE-306: Missing Authentication for Critical Function) and (c) declassification-function (downgrading, the reverse of confidential operations)) using UML state charts. Next, the obtained UML state charts will be annotated using our light-weight security annotation language. If needed the light-weight annotation language will be extended to deal with the new scenarios. Next, C code will be generated which will be statically analysed using our symbolic execution engine. Needed C code generator extensions should be taken into consideration and implemented. The three types of checkers for a, b and c will be implemented inside our symbolic execution engine. Needed information flow inference rules will be formally defined and implemented. The inference rules will be implemented by following the principle of 'low coupling and high cohesion' inside our engine architecture. Checker bug reports will be presented in the Eclipse 'Problems' view and error traces will be depicted as UML sequence diagrams.

**Requirements**

Very good Java programming skills, Eclipse CDT/EMF/xText/xTend knowledge, Secure information flow propagation knowledge is an advantage

**Contact**

M.Sc. Paul Muntean,
E-Mail: paul@sec.in.tum.de,
Tel.: (089) 289-18566,
Tender date: April 20, 2015,
Beginning: 01.05.2015