

Sujet de stage de recherche / M2

Titre

Estimating the information leakage of a probabilistic recursive program

Encadrants

Rohit Chadha & Stefan Schwoon

Tél : 01 47 40 22 72 & 01 47 40 75 63

Web : <http://www.lsv.ens-cachan.fr/~home{chadha}> & *Web* : <http://www.lsv.ens-cachan.fr/~home{schwoon}>

Email : chadha@lsv.ens-cachan.fr & schwoon@lsv.ens-cachan.fr

Laboratoire Spécification et Vérification

École Normale Supérieure de Cachan

61, avenue du Président Wilson

94235 Cachan CEDEX

Description du sujet

Several programs input sensitive secret data such as passwords and PINS; while outputting less sensitive. A central problem in computer security is to measure the amount of the sensitive input information an attacker can learn from observing the output. The information-theoretic measure of mutual information has been proposed as a measure as the information leaked by such a program (see [Smi09], for example) : the amount of information leaked by a program P is the mutual information between the input distribution and the output distribution.

In order to compute this measure one has to compute for each input x and output y , the conditional probability $pr(output = y | input = x)$. Two methods have been proposed in the literature to achieve the latter. One is to employ statistical methods by generating enough sample size to estimate the conditional probability. Another method is to employ model-checking techniques to calculate it explicitly using model-checking techniques.

The primary objective of the internship would be to explore the use of model-checking techniques to compute the information-leakage when the programs are both recursive and probabilistic. For such programs, the probability $pr(output = y | input = x)$ can be approximated using a set of polynomial equations over the field of reals. However, in practice Newton's method in which the solutions are approximated by iterative methods are employed [WE07]. The main challenge in the application of Newton's method is state space explosion. The number of states of such programs can

be huge resulting in slow convergence of Newton's method. In order to overcome this problem, we will combine symbolic model-checking techniques with Newton's method. We expect the developed techniques to automatically find attacks in recursive probabilistic programs.

Remarques

We are looking for candidates with good skills in Foundations of Computer Science (algorithms, data structures, automata theory . . .), programming and basic mathematics (probability theory, multivariate-calculus). Some knowledge in security is an asset but is not mandatory.

Références

- [Smi09] Geoffrey Smith. On the foundations of quantitative information flow. In *Foundations of Software Science and Computational Structures, 12th International Conference (FOSSACS)*, volume 5504 of *Lecture Notes in Computer Science*, pages 288–302, 2009.
- [WE07] D. Wojtczak and K. Etessami. Premo : An analyzer for probabilistic recursive models. In *Tools and Algorithms for the Construction and Analysis of Systems, 13th International Conference (TACAS)*, volume 4424 of *Lecture Notes in Computer Science*, pages 66–71. Springer, 2007.