2018-01129 - Postdoc: Symbolic tools for the formal verification of cryptographic protocols

Renewable contract : Oui
Level of qualifications required : PhD or equivalent
Fonction : Post-Doctoral Research Visit

Context
A 12-month position for post-doctoral research on
Symbolic tools for the formal verification of cryptographic protocols
is available at the Inria Nancy / LORIA research center within the Inria project team

PESTO: Proof techniques for security protocols [1]
as part of the ERC Grant

Assignment
Security protocols are distributed programs that aim at ensuring security properties, such as confidentiality, authentication or anonymity, by the means of cryptography. Such protocols are widely deployed, e.g., for electronic commerce on the Internet, in banking networks, mobile phones and more recently electronic elections. As properties need to be ensured, even if the protocol is executed over untrusted networks (such as the Internet), these protocols have shown extremely difficult to get right. Formal methods have shown very useful to detect errors and ensure their correctness.

One generally distinguishes two families of security properties: trace properties and observational equivalence properties. Trace properties verify a predicate on a given trace and are typically used to express authentication properties. Observational equivalence expresses that an adversary cannot distinguish two situations and is used to model anonymity and strong confidentiality properties.

The Tamarin prover [3] is a state-of-the art protocol verification tool which has recently been extended to verify equivalence properties in addition to trace properties. SAPIC [4] allows protocols to be specified in a high-level protocol specification language, an extension of the applied pi-calculus, and uses the Tamarin prover as a backend by compiling the language into multi-set rewrite rules, the input format of Tamarin. TAMARIN and SAPIC have been successfully used to verify standards such as TLS 1.3 and 5G ANX as well as industrial protocols such as OPC UA. The objective of this postdoc is to contribute to the development of the SAPIC/Tamarin toolchain, work on extensions and use the tool(s) to analyze particular classes of protocols.

Main activities
Research
Skills
Applications, including
- a motivation letter including your scientific and career projects,
- a CV describing your research activities (max. 2 pages),
- a short description of your best contributions (max. 1 page for max. 3 contributions including theoretical research, implementation or industry transfer),
- your two best publications,
- if you have not defended yet, the list of expected members of your PhD committee and the expected date of defense,

should be sent to jannik.dreier@loria.fr and steve.kremer@inria.fr as two pdf files (one for the publications, the other for the other documents).

Additionally, at least one recommendation letter from your PhD advisor(s), and up to two additional letters of recommendation should be sent directly by their authors to the email addresses indicated above.

Applications should be received by June 30, 2019, but applications received later may still be considered.

Informal enquiries concerning the position are welcome.

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours
- Sports facilities

General Information
- Theme/Domain : Security and Confidentiality
- Town/city : Villers-lès-Nancy
- Inria Center : CRI Nancy - Grand Est
- Starting date : 2019-09-01
- Duration of contract : 1 year
- Deadline to apply : 2018-12-31

Contacts
- Inria Team : PESTO
- Recruiter : Dreier Jannik / jannik.dreier@loria.fr

About Inria
Inria, the French national research institute for the digital sciences, promotes scientific excellence and technology transfer to maximise its impact. It employs 2,400 people. Its 200 agile project teams, generally with academic partners, involve more than 3,000 scientists in meeting the challenges of computer science and mathematics, often at the interface of other disciplines. Inria works with many companies and has assisted in the creation of over 160 startups. It strives to meet the challenges of the digital transformation of science, society and the economy.

The keys to success
Successful candidates must have defended a PhD in computer science, or expect to defend their PhD before taking up the position. Expected qualifications are:
- solid knowledge of logic, proofs and/or formal verification techniques,
- solid programming experience, ideally with functional programming in OCAML or Haskell.

Security knowledge is not required, but a plus.

Conditions for application
Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy : As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.
Remuneration
2 653 euros brut / month