2023-06577 - PhD Position F/M Dolev-Yao model-guided fuzzing of cryptographic protocols

Contract type: Fixed-term contract
Renewable contract: Yes
Level of qualifications required: Graduate degree or equivalent
Function: PhD Position
Level of experience: Recently graduated

Context
- **Topic:** Security, Cryptology, Cybersecurity, Verification, Fuzzing
- **Location:** The thesis will be located at Inria Nancy (Université de Lorraine) in Nancy, France.
- **Team:** The inria PESTO team (https://team.inria.fr/pesto/)
  - Advisors: Luca Hirschi, Luca.Hirschi@inria.fr and Steve Kremer, Steve.Kremer@inria.fr
  - Funding: The project is supported by the ANR JCJC project ProtoFuzz.

Assignment
**General Context.** Cryptographic protocols are distributed programs that aim at ensuring secure 7 weeks of use 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 and dedicated tools such as ProVerif or Tamarin, have shown very useful to detect errors and ensure their correctness at the level of protocol specifications. However, specifications are simply an abstraction of the program that end-users deploy and run, and are themselves plagued with frequent implementation bugs.

**Objectives.** The goal of this PhD thesis is to contribute to the DY Fuzzing project. This project proposes a novel and effective technique that we call Dolev Yao (DY) model-guided fuzzing, which precludes logical attacks against protocol implementations. The main idea is to consider as possible test cases the set of abstract DY executions of the DY attacker, and use a mutation-based fuzzer to explore this set. A first description of these ideas and a prototype implementation of a DY fuzzer are given in [1]. This first paper paves the way for a large number of follow-up works: plugging the fuzzer of different TLS implementations, designing a fuzzer for other protocols (e.g. DTLS, QUIC, WPA, ...), designing better metrics to guide the fuzzer among others.


Main activities
- Study of cryptographic protocol implementations
- Designing more effective techniques for DY fuzzing
- Implementation and evaluation of these techniques
- Writing scientific papers
- Presentation of results in seminars and conferences

Skills
In addition to mathematical maturity, the candidate must be able to contribute to the development of an open source project. A good command of Rust and collaborative developing environments (git) would be welcome. Familiarity with formal verification tools, in particular for protocol verification are not mandatory but considered a plus.

Benefits package
- Subsidized meals
- Partial reimbursement of public transport costs
- Leave 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration
Salary: 2082€ gross/month for 1st and 2nd year. 2190€ gross/month for 3rd year.

General Information
- **Theme/Domain:** Security and Confidentiality
- **Software engineering (BAP E)**
- **Town/city:** Villers lès Nancy
- **Inria Center:** CB Nancy - Grand Est
- **Starting date:** 2023-11-01
- **Duration of contract:** 3 years
- **Deadline to apply:** 2023-08-31

Contacts
- Inria Team: PESTO
- PhD Supervisor: Kremer Steve / Steve.Kremer@inria.fr

About Inria
Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success
The candidate is expected to have mathematical maturity, should be curious and open to learning new subjects. Good communication skills and the ability to work in a team are also essential.

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.

Instruction to apply
**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). Authorization 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.