2018-00411 - Post-doctoral - Development of Unbreakable Shared-Key Cryptography Protocols

Contract type: Public service fixed-term contract
Renewable contract: Oui
Level of qualifications required: PhD or equivalent
Fonction: Post-Doctoral Research Visit
Level of experience: Recently graduated

Context

The TAMIS team at Inria Rennes - Bretagne Atlantique is among the largest security teams at Inria, including competences from hardware attacks to cryptography, and from vulnerability detection to malware analysis. This project is connected to the Chair of Cybersecurity in Threat Analysis financed by Région Bretagne.

Assignment

Shared-key cryptography consists of covert communications between two agents that possess a pre-shared key that is unknown to the attacker. The information-theoretical analysis of such protocols has been pioneered by Shannon in the 1940s and developed ever since. In particular, Shannon introduced the concept of perfect secrecy, that is, mathematical proof that a protocol does not leak any information about the message transmitted through the hidden channel. The one-time pad protocol has been proved to have perfect secrecy under reasonable conditions over the message and key, and has been used in many high-security applications. However, Shannon proved that for a protocol to have this property the message sent cannot be longer than the pre-shared key, and the key itself can be used only once.

Recently, a breakthrough in this field by our team has been the definition of max-equivocation, a generalization of perfect secrecy that exactly characterizes the maximum amount of possible secrecy that can be guaranteed by any protocol for given key and message distributions. Contrarily to perfect secrecy, it is possible to build shared-key cryptographic protocols that use a key significantly shorter than the message and where it is allowed to reuse the key an unlimited amount of times. We have developed such protocols and proven mathematically their unbreakableness and their optimality, following and expanding on Shannon's research. Additionally, we have created a new class of shared-key cryptosystems called Apollonian encoders, that are always guaranteed to achieve max-equivocation, and thus mathematically optimal on a very large class of entropy measures.

However, in practice communication protocols need to preserve additional interesting properties, like tampering detection, man-in-the-middle resistance, and authentication. To be integrated in an unbreakable communication protocol they need to not be relying on computational assumptions on the attacker, instead being resistant against an unconditional attacker assumed to have unlimited computational power.

Main activities

Tampering detection against an unconditional attacker can be guaranteed using encrypted hashes. However, obtaining this without consuming the key is still an open problem. Similar techniques can be adapted to detect out-of-order transmission or packet drops by man-in-the-middle attackers.

Authentication against unconditional attacker can be obtained adapting Wegman-Carter authentication schemes, again considering the consequences to key consumption.

The candidate will work on developing a complete and unbreakable shared-key communication protocol, including mathematically proving that the protocol has the properties of interest and developing a reference implementation in the C language to allow for further development and standardization. A calendar of the proposed contributions follows:

- **6 months**: state of the art of unconditional cryptography; information-theoretical formalization of properties of interest (tampering detection, authentication, etc.)
- **12 months**: preliminary results for unconditionally-secure communication protocol submitted to a security conference rated at least A (IEEE S&P, CSF, TrustCom, etc.), prototype protocol with properties of interest, proof of impossibility for properties of interest not included

General Information

- Theme/Domain: Security and Confidentiality
- Town/city: Rennes
- Inria Center: CRI Rennes - Bretagne Atlantique
- Starting date: 2018-10-01
- Duration of contract: 1 year, 6 months
- Deadline to apply: 2018-05-15

Contacts

- Inria Team: TAMIS
- Recruiter: Biondi Fabrizio / fabrizio.biondi@inria.fr

The keys to success

Active mind, problem-solving attitude, professionalism

Conditions for application

Please submit online: your resume, cover letter and letters of recommendation.

For further information, please contact Fabrizio Biondi (fabrizio.biondi@inria.fr)

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.
18 months: final version of the protocol published in security conference as above, reference implementation ready and published

Skills
The candidate should feel comfortable working on research in a team environment. Good communication and programming skills are highly valued. Knowledge of probability theory, information theory, and cryptography will be strongly considered.

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

Remuneration
Monthly gross salary amounting to 2653 euros