Offer #2025-09154

Post-Doctoral Research Visit F/M Decentralised Public Key Infrastructure

Contract type : Fixed-term contract

Level of qualifications required : PhD or equivalent

Fonction : Post-Doctoral Research Visit

Context

This postdoc position will be in the context of IPCEI-CIS (Important Project of Common European Interest – Next Generation Cloud Infrastructure and Services) DXP (Data Exchange Platform) project involving Amadeus and three Inria research teams (COAST, CEDAR and MAGELLAN). This project aims to design and develop an open-source management solution for a federated and distributed data exchange platform (DXP), operating in an open, scalable, and massively distributed environment (cloud-edge continuum).

The postdoc will be located at The Inria Center of the University of Lorraine in the COAST team.

The Inria Center of the University of Lorraine is one of Inria's nine centers and has twenty project teams, located in Nancy, Strasbourg and Saarbrücken. Its activities occupy over 400 people, scientists and research and innovation support staff, including 45 different nationalities. The Inria Center is a major and recognized player in the field of digital sciences. It is at the heart of a rich R&D and innovation ecosystem: highly innovative PMEs, large industrial groups, competitiveness clusters, research and higher education players, laboratories of excellence, technological research institutes, etc.

Assignment

Some End-to-End Encryption (E2EE) systems leverage out-of-band (OOB) channels for client authentication, using either manual comparison of public key fingerprints [1] or pre-shared passwords [2].

However, a secure and user-friendly OOB channel is difficult to implement in practice. Users often overlook password entropy, while fingerprint comparison is error-prone and tedious [3].

Other client authentication solutions rely on trusted third parties, i.e., key servers, to distribute and authenticate public keys between clients. Many popular E2EE

services such as WhatsApp [4] use centralized key servers because they are easy to use and simple to implement. However, a centralized key server becomes a single point of failure, vulnerable to attacks from adversaries or surveillance agencies. As a result, achieving secure and autonomous client authentication remains a major challenge for E2EE.

Rather than preemptively verifying exchanged keys, key transparency [5][6][7] allows clients to verify whether the key server is behaving correctly during communication. The general idea is to turn the key server into a transparent logging server using an authenticated data structure [8] that is append-only and thus efficiently auditable. The key server acts as a prover, returning public keys upon request along with compact proofs that can be verified by the clients. This way, clients are not concerned about Man-In-The-Middle (MITM) attacks, as any attempt to tamper with client keys is logged in an auditable server log.

The authenticated data structure guarantees that the server cannot modify user keys without being recorded. However, a compromised key server could still behave inconsistently by presenting different responses to different clients. Therefore, logging clients need a way to cross-validate the information they receive to ensure key server consistency across clients. This process is known as auditing. There are third-party clients (auditors) that regularly query the key server for proofs. Thus, whenever clients receive responses from the key server, they can verify the proofs using these auditors. The state of the art recommends using a gossip protocol between logging clients and auditors to share information and efficiently blacklist any compromised key server.

However, such a gossip protocol is difficult to implement in practice [8]. It is vulnerable to certain failure modes in adversarial networks, such as Sybil attacks [9]. It is hard to incentivize clients to participate and bootstrap the gossip network. Furthermore, user privacy may be at risk [10]. To date, there is no known complete protocol design for gossiping in current transparent logging systems. A similar effort in the area of certificate transparency [11] is currently under standardization, although after several years, it is still not finalized.

Rather than using a separate gossip protocol, EthIKS [12] implements the transparent log server on the Ethereum blockchain [13]. However, because EthIKS's operational cost increases with the number of users, and due to the significant rise in the price of ETH, the system does not scale well to large key servers with millions of users.

We aim to propose an efficient decentralized public/private key infrastructure enabling the verification of the authenticity of asymmetric key pairs, thereby preventing man-in-the-middle attacks.

References:

[1] Zimmermann, P.R.: The official PGP user's guide. MIT press (1995)
[2] Boyko, V., MacKenzie, P., Patel, S.: Provably secure password-authenticated key exchange using diffie-hellman. In: Advances in Cryptology - Eurocrypt 2000. pp. 156–171. Springer (2000)
[3] Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX Security Symposium. vol. 348 (1999)
[4] WhatsApp: WhatsApp Messenger. https://www.whatsapp.com/ (2017), accessed on 28.08.2017

[5] Google: Key Transparency. https://github.com/google/keytransparency (2017)
[6] Melara, M.S., Blankstein, A., Bonneau, J., Felten, E.W., Freedman, M.J.: Coniks: Bringing key transparency to end users. In: 24th USENIX Security Symposium (USENIX Security 15). pp. 383–398 (2015)
[7] Yahoo: Yahoo End-To-End. https://github.com/yahoo/end-to-end (2017)
[8] Birman, K.: The promise, and limitations, of gossip protocols. ACM SIGOPS Operating Systems Review 41(5), 8–13 (2007)
[9] Douceur,J.R.: The sybil attack. In: International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002)
[10] Nordberg, L.: Gossiping in CT. https://tools.ietf.org/html/draft-linus- trans-gossip-ct-00 (2014)
[11] Laurie, B.: Certificate transparency. Queue 12(8), 10:10–10:19 (Aug 2014). https://doi.org/10.1145/2668152.2668154, http://doi.acm.org/10.1145/2668152.2668154
[12] Bonneau, J.: Ethiks: Using ethereum to audit a coniks key transparency log. In: International Conference on Financial Cryptography and Data Security. pp. 95–105. Springer (2016)
[13] Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151, 1–32 (2014)
[14] Julia Len, Melissa Chase, Esha Ghosh, Kim Laine, and Radames Cruz Moreno. 2024. OPTIKS: an optimized key transparency system. In Proceedings of the 33rd USENIX Conference on Security Symposium (SEC '24). USENIX Association, USA, Article 244, 4355–4372.
[15] Nguyen, H. L., Ignat, C. L., and Perrin, O. Trusternity : Auditing transparent log server with blockchain. In Companion Proceedings of The Web Conference 2018 (pp. 79-80).

Main activities

- Analysis of the existing state of the art on key transparency [5][6][7][14] and decentralised public key infrastructures
- Analysis of Trusternity [15] (https://github.com/coast-team/coniks-go, https://github.com/coast-team/trusternity-contract/), an extension of CONIKS [7]. Trusternity replaces the gossiping mechanism used in CONIKS with an implementation of the synchronization and audit mechanism based on smart contracts on the Ethereum blockchain.
- Proposal of a decentralized public key infrastructure
- Prototype of the proposed infrastructure

Skills

- PhD in Computer Science
- Fundamentals of Distributed systems and blockchain technology (smart-contract)
- Fundamentals of Applied Cybersecurity (symmetric and asymmetric cryptography, access control, authorization)
- Good programming skills
- Good collaborative and networking skills, excellent written and oral communication in English
- Strong analytical skills

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

€2788 gross/month

General Information

- **Theme/Domain :** Distributed Systems and middleware
  System & Networks (BAP E)
- **Town/city :** Villers lès Nancy
- **Inria Center :** Centre Inria de l'Université de Lorraine
- **Starting date :** 2025-10-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2025-08-15

Contacts

- **Inria Team :** COAST
- **Recruiter :**
  Ignat Claudia-lavinia / claudia.ignat@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.

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).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.