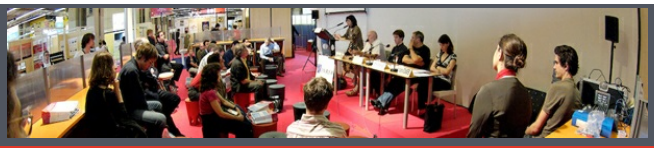
INTERNATIONAL RELATIONS



INTERNSHIP SUBJECT

109 - Analysis of the W3C Web Crypto API Key Management Mechanism

The W3C is currently standardising an API for cryptography in web applications that will be implemented by all the major browser vendors. This is a major advance in web security: currently web applications have to perform their cryptography in javascript which creates a number of security problems. However designing such APIs is a far from trivial task: finding flaws in such APIs and then verifying their fixes has been a major subject for research in the INRIA PROSECCO team.

Harry Halpin, head of the W3C working group on the crypto API recently contacted the PROSECCO team to ask for an audit of the proposal, with special attention to the key management commands. This we will do by designing a small formal model and verifying it with our tools. This model may then be used to help generate the standard javascript test suite for the API. The W3C consider this work to be highly important for future security on the web (their letter of interest backs this up).

The intern who will carry out the work under the supervision of PROSECCO researchers should be comfortable with basic notions in cryptography and formal modelling.

Required Skills

Cryptography

Security APIs

Formal Modelling

Javascript

General Information

- **Research Theme :** Security and Confidentiality
- **Locality :** Le Chesnay
- **Level :** PhD
- **Period :** 1st March 2014 -> 31st May 2014 (3 months)

  These are approximative dates. Please contact the training supervisor to know the precise period.

- **Deadline to apply :** 22nd December 2013 (midnight)

Contacts

- **Training Supervisor :** Graham Steel / Graham.Steel@inria.fr
- **Second Training Supervisor :** Bhargavan Karthikeyan / karthikeyan.bhargavan@inria.fr
- **Team Manager :** Bruno Blanchet / Bruno.Blanchet@inria.fr

More information

- **Inria Team :** PROSECCO
- **Inria Center :** Centre Inria de Paris