Malware classification through side-channel information: Engineering or PostDoc Position

Research topic While malware detection and mitigation research is now trending, a lot of challenges and unsolved problems still remain. Recently, sophisticated malware designers invented techniques to circumvent software detection techniques, which make them unreliable in practice. A new direction consists in using unintentionally emitted hardware side-channel information such as electromagnetic emanation, power consumption, timing, performance counters as mechanism to detect malware. The big advantage of this information is the non-detection by malware designers. Still, those approaches have to be established in real-world scenarios and efficient analysis techniques developed and implemented.

We are currently building up a *realistic IoT malware side-channel analysis platform* which gives us first interesting new insights.

Joining our team you will

- infect IoT devices with malware,
- be responsible for the maintenance of the side-channel workbench,
- derive and develop efficient implementations of analysis algorithms,
- drive top-quality research and publish in A*/A-class security and malware conferences.

Prerequisites We are looking for team players who are motivated and able to drive top-quality research. The area of research lies between several fields and we expect at least competences in one of them:

- embedded devices/side-channel analysis, and/or
- statistics, machine learning, deep learning, and/or
- malware analysis.

Additionally an ideal candidate should have:

- Research engineer: MS degree in Computer Science, Computer Engineering, Electrical Engineering, or related fields, with 1-3 years work experience,
- PostDoc: PhD in Computer Science, Computer Engineering, Electrical Engineering, or related fields
- good programming skills,
- good level in written and spoken English,
- motivation to save the world.

Environment The TAMIS team at IRISA, Inria Rennes - Bretagne Atlantique mainly focuses on vulnerability analysis ranging from software to hardware attacks, with a strong focus on malware classification and side-channel analysis.

Duration/Starting date The position is initially limited to one year but can be extended (up to two years) in case of good performance. The starting date is as soon as possible (given our security clearances).

Contact Interested candidates should send their detailed CV, cover letter and references to Annelie Heuser, annelie.heuser@irisa.fr.