Non-Invasive Attack Testing Workshop (NIAT 2011)

Nara, Japan

Reception: Sunday 25 September
Workshop Sessions: Monday September 26 – Tuesday September 27

Call for Papers

The Cryptographic Module Validation Program (CMVP) and AIST are organizing a workshop in support of developing test methods, metrics and tools for performing repeatable conformance testing of mitigations against non-invasive attacks on cryptographic modules. The workshop will take place prior to and share a venue with CHES 2011.

Non-invasive attacks are performed on cryptographic devices without physical contact. As the information security community addresses the increasing threat of non-invasive attacks, and requirements addressing these attacks are incorporated into security standards, reliable and repeatable test methods, test metrics and test tools for determining compliance to those requirements must also be developed. The aim of the workshop is to attract researchers and developers from academia, industry and test laboratories to discuss topics relating to non-invasive attack testing.

The CMVP validates cryptographic modules for conformance to NIST FIPS PUB 140-2 (and its successors). The CMVP is a joint program between NIST and the Communications Security Establishment Canada (CSEC).

The NIAT Workshop encourages submissions on any topic related to non-invasive attack testing. This includes, but is not limited to:

- Non-Invasive Attacks against NIST Approved Algorithms (FIPS 140-2 Annex A)
- Non-Invasive Attack Testing Schemes, Methods, Metrics and Tools for SPA, DPA, EMA and Timing Attacks
- Countermeasures

Important Dates

Submission Deadline	August 5, 2011 (Closed)
Author Notification	August 12, 2011 (Completed)
Final Version Due	September 19, 2011 (Extended)
Workshop	September 25-27, 2011

Instructions for Authors

Authors are invited to submit abstracts for original papers via email. A submission should include a title, the author's name, a short abstract, and a list of keywords. The abstract should be at most 1 page, single spaced, with 1 inch margins using a 10pt or larger font in plain-text or PDF format. The authors of the submitted papers guarantee that their paper will be presented at the workshop if their abstract is accepted. All submissions will be acknowledged.
Please submit abstracts to **non-invasive@nist.gov**

Final papers should be provided electronically, in PDF, for standard US letter-size or international A4-size paper. Submitted papers must not exceed 15 pages (single space, with 1 inch margins using a 10 pt or larger font). Please send the following information to **non-invasive@nist.gov**

- Name, affiliation, email, phone number, postal address for the primary submitter
- Name and affiliation of each co-submitter
- The finished paper in PDF format as an attachment