To: submissions@nspw.org
cc: George Robert Blakley III/Austin/IBM@IBMUS, jmchugh@cert.org, h.lim@rhul.ac.uk
Subject: Paper submission for NSPW 2005

Dear Program Chairs,

Please find attached a copy of my paper which I hope to be considered for the NSPW 2005. The required information about my submission is as follows.

1. Category: Position paper
2. Attendance statement: If the paper is accepted, Hoon Wei Lim will attend the workshop.
3. Justification for inclusion:

Many emerging technologies for distributed computing systems such as pervasive and Grid computing require rather heavyweight key management through the conventional PKI approach. This is mainly due to some unique security requirements of the emerging distributed systems which require regular involvement of users in managing their public keys (e.g. generation, update, distribution, and etc.) and certificates (e.g. generation, renewal, revocation, and etc.). For an average or low-end user platform, this may seem to be considerably expensive in terms of computational power and network bandwidth.
We propose a new paradigm which emphasises on unification of public key management that may result a more lightweight and flexible key infrastructure.
Through the use of "static certificate" and "master-public-key mould", the users can cut down extensive use of certificate and enjoy simpler non-interacitve public key update which may seem to align well with some of the distinct security requirements for the emerging distributed systems such as single sign-on and credentials delegation. In addition, the master-public-key mould can be used to produce different kinds of dynamic public keys which can have different roles such as long-term, short-term, and secret, without acquiring any additional certificates that validate these keys.

Through the workshop, we hope to discuss and debate with other participants about the practicality of our proposal and also potentially identify some other
interesting applications of this approach which are unspecified in the paper.

Cheers,
Hoon Wei

- DKI v2.0.pdf