

Protecting Mobile Devices Against Loss and Capture

Speaker: Zhengyi Le, Heracleia Lab, CSE@UTA

Date: Friday, March 28, 2008

Time: 10:00-11:00 am

Venue: WH 413 (Woolf Hall)

Abstract:

Mobile devices play a critical role in assistive environments. How to authenticate them and secure communications among them has been an important problem, especially against loss and capture. We present an approach to protect signing keys of mobile devices based on mediated RSA introduced by Dan Boneh and others. The important property of our scheme is transparent self-resilience. In other words, in case a device is lost or captured and at the risk of being compromised and impersonated, our scheme can disable the device instantly and the replacement will be transparent to other users. In this way, if an attacker captures a mobile device, he has a limited time to use it because it will become invalid soon. If he wants to break our scheme, he must compromise the device and its mediator simultaneously.

Biography:

Zhengyi Le is receiving her Ph.D. majored in Computer Science at Dartmouth College, under the direction of Prof. Fillia Makedon. She is currently a senior researcher and the assistant director of Heracleia Lab at the University of Texas at Arlington.