[edit] Presentation Abstracts

[edit] (U) Times

(U) Each day will run from 9am to 5pm. In order to facilitate planning, the topics presented on each day are highlighted below. The abstracts for each topic are on the following pages.

[edit] Tuesday, 16 March

[edit] (S//NF/ORCON) TPM Vulnerabilities to Power Analysis and an Exposed Exploit to Bitlocker

(U) Presenter: [redacted]

(S//NF/ORCON) Power analysis, a side channel attack, can be used against secure devices to non-invasively extract protected cryptographic information such as implementation details or secret keys. We have employed a number of publically known attacks against the RSA cryptography found in TPMs from five different manufacturers. We will discuss the details of these attacks and provide insight into how private TPM key information can be obtained with power analysis. In addition to conventional wired power analysis, we will present results for extracting the key by measuring electromagnetic signals emanating from the TPM while it remains on the motherboard. We will also describe and present results for an entirely new unpublished attack against a Chinese Remainder Theorem (CRT) implementation of RSA that will yield private key information in a single trace.

(S//NF/ORCON) The ability to obtain a private TPM key not only provides access to TPM-encrypted data, but also enables us to circumvent the root-of-trust system by modifying expected digest values in sealed data. We will describe a case study in which modifications to Microsoft's Bitlocker encrypted metadata prevents software-level detection of changes to the BIOS.