

An Introduction to Side Channel Analysis: SPA, DPA and Timing Attacks

1-day Tutorial by Cryptography Research
9 am – 5 pm, 14 August, 2008

Crowne Plaza Washington DC/Silver Spring
8777 Georgia Avenue, Silver Spring, MD 20910

Agenda

Session 1: Timing Attacks & Simple Power Analysis (SPA)

- Introduction to timing attacks
- Interactive PIN verify attack using timing leak
- Introduction to SPA
- Interactive PIN verify attack using SPA
- SPA waveform analysis exercise

Session 2: Differential Power Analysis (DPA)

- Introduction to DPA
- Demo: DPA attack on embedded microcontroller
- Overview of advanced DPA topics

Session 3: Hands-on SPA Analysis

- Introduction to DPA Workstation
- Hands-on exercise: Recover an RSA exponent using SPA

Session 4: Countermeasures & Certification Issues

- SPA/DPA countermeasures
- Specifying and certifying DPA resistance

Speakers

- Benjamin Jun Vice President of Technology
- Josh Jaffe Cryptosystem Researcher and Engineer