Rambus
Cryptography Research

Sample Agenda (subject to revision):

Day 1

9:00 – 9:15

Welcome and Overview of Rambus Cryptography Research and Workshop (15 min)

Who we are and what we do.

9:15 – 10:15

Simple Power Analysis (SPA) (60 min)

Introduction to correlating device power usage with its operation by inspection.

10:15 – 10:30

Break

10:30 – 11:00

SPA Exercise (PIN, waveform identification) (30 min)

Extract a PIN using SPA from a device simulator. Associate a collection of power trace waveforms with the algorithms that generated them.

11:00 – 11:45

SPA/EM Demonstration (45 min)

Demonstrate SPA techniques by monitoring power usage inferred through EM propagation.

11:45 – 12:45

Lunch

12:45 – 13:45

SPA Modular Exponentiation Exercise (60 min)

Recover a portion of an RSA exponent by applying SPA techniques.

13:45– 14:45

Differential Power Analysis (DPA) (60 min)

Introduction to correlating device power usage with its operation using statistical methods.

14:45 – 15:00

Break

15:00 – 15:30

DPA Demonstration (30 min)

Demonstrate DPA techniques by extracting the key from FPGA fabric and bitstream.

15:30 – 15:45

Differential Power Analysis Workflow and Tutorial Introduction (15 min)

Presentation of differential power analysis tools.

15:45 – 17:00

Differential Power Analysis Tutorial (75 min)

Recover a portion of an AES key by applying DPA.

Rambus
Cryptography Research

Day 2

9:00 – 9:30
DPA on AES Counter Mode (30 min)
DPA of AES in Counter Mode describing key extraction without knowledge of messages

9:30 – 10:30
DPA on SHA Family in Key Derivation (60 min)
Lecture and demonstration of DPA of keyed SHA family hash

10:30 – 10:45
Break

10:45 – 11:45
Advanced Lecture: ECC (60 min)
Examination of ECC implementation vulnerabilities

11:45 – 12:00
Host Presentation (15 min)
TSA, Inc Service Offerings

12:00 – 13:00
Lunch

13:00 – 14:00
Preventing DPA: Countermeasures (60 min)
Survey of approaches to countering DPA and their tradeoffs.

14:00 – 14:45
Testing and Certification: Validating and Evaluating Devices (45 min)
Review side-channel resistance requirements in existing standards, guidance for conformance testing.

14:45 – 15:00
Break

15:00 – 15:15
DPA Product Offerings – DPARC/DPASL/DPAWS (15 min)
A review of the analysis platform and DPA-resistant hardware and software solutions.

15:15 – 16:00
TVLA and Countermeasure Demonstration (45 min)
Demonstration of Test Vector Leakage Assessment (TVLA) of protected and unprotected AES cores.

16:00 – 17:00
Discussion / Wrap-up / Q&A (60 min)