Sample 2-day Agenda:
Side-Channel Analysis Workshop

Day 1

9:00- 9:15
Welcome and Overview of Rambus Cryptography and Workshop (15 min)

9:15 - 10:30
Simple Power Analysis (75 min)

9:15 - 10:00	Introduction to SPA
10:00 - 10:15	SPA Waveform Analysis Exercise
10:15 - 10:30	Interactive PIN Verify Attack

10:30- 10:45
Break

10:45 - 11:45
SPA Modular Exponentiation Exercise (60 min)
Exercise recovering an RSA exponent using SPA

11:45 - 12:15
Electromagnetic Analysis Demonstration (30 min)
Live demonstration on a variety of devices showing side-channel leakage and its exploitation

12:15- 12:45
Lunch
Product Solutions for DPA/Fault attacks discussion

12:45 - 15:00
Differential Power Analysis (135 min)

12:45 – 13:45	Introduction to DPA
13:45 – 14:00	Demo: DPA Key Extraction on an FPGA
14:00 – 15:00	Hands-on exercise

15:00- 15:30
Preventing DPA: Countermeasures (30 min)

15:30 - 15:45
Break

15:45 - 16:00
DPA Product Offerings (15 min)
A review of Rambus Cryptography's analysis platform and DPA-resistant hardware and software solutions.

16:00 - 16:30
Advanced Topics in DPA (30 min)
Demonstration of advanced DPA techniques

16:30- 17:15
Testing and Certification: Validating and Evaluating Devices (45 min)
Review of side-channel requirements in existing standards (FIPS, Common Criteria, PCI, etc.) and recommendations for conformance testing.

Day 2

9:00 – 9:30
Riscure Intro – 30min

9:30 – 10:00
Deep Learning – 30min

10:00 – 10:30
Thinking Like an Attacker: An Attacker's Point of View – 30min

10:30 – 10:45
Break

10:45 – 11:30
Introduction into Fault Injection – 45min

11:30 – 12:00
Inspector FI in Python – 30 min

12:00 – 12:45
Lunch

Product Solutions for DPA/Fault attacks discussion, covering Anti-tamper, hardware root of security, and secure supply chain

12:45– 13:45
Hands-on Fault Injection

13:45 – 14:15
Fault Injection – Hardware and Software Simulation – 30min

14:15 – 15:00
Secure Boot – 45min

15:00 – 15:15
Break

15:15 – 16:00
Source Code Analysis Tool (TCAT) – 45min

16:00 – 16:45
Demo's and challenge – 45min

16:45 – 17:00
Q&A Wrap-up – 15-30min