Introduction to Trusted Computing: Course Overview

Ariel Segall
ariels@alum.mit.edu

Spring 2012

License

All materials are licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

to make commercial use of the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

A Note for Open Security Training Users

The slides for this course were revised between the recorded session and now. In order to provide the best materials, the revised slides have been included here; however, you may notice some discrepancies between the recordings and the slides. I apologize; if I ever have the chance to rerecord the video, I will.

Day 1

- Quick Crypto and Security Vocabulary Review
- What Is Trusted Computing?
- TPM 101: A High Level Summary
- Trusted Computing Ecosystem: Beyond the TPM
- Lunch!
- Trusted Computing in the Enterprise: Where We Are Today and Where We're Going
- TPM Provisioning
- TPM Keys: Creating Them, Certifying Them, and Using Them

Day 2

- Using the TPM: Machine Authentication and Attestation
- Using the TPM: Data Protection and Storage
- Using the TPM: Other Capabilities
- Lunch!
- From Theory to Reality
- Resources for Further Investigation

About This Class

- Ask questions early and frequently!
  - Concepts build on each other
- Discussion encouraged
  - Section of second afternoon reserved for student questions and use cases
- Schedule may vary!