Introduction to Trusted Computing:
Course Overview

Ariel Segall
ariels@alum.mit.edu

Spring 2012

Approved for Public Release: 12-2749.
Distribution unlimited
All materials are licensed under a Creative Commons “Share Alike” license.

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