Advanced x86:
BIOS and System Management Mode Internals
Introduction

Xeno Kovah && Corey Kallenberg

LegbaCore, LLC

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

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).

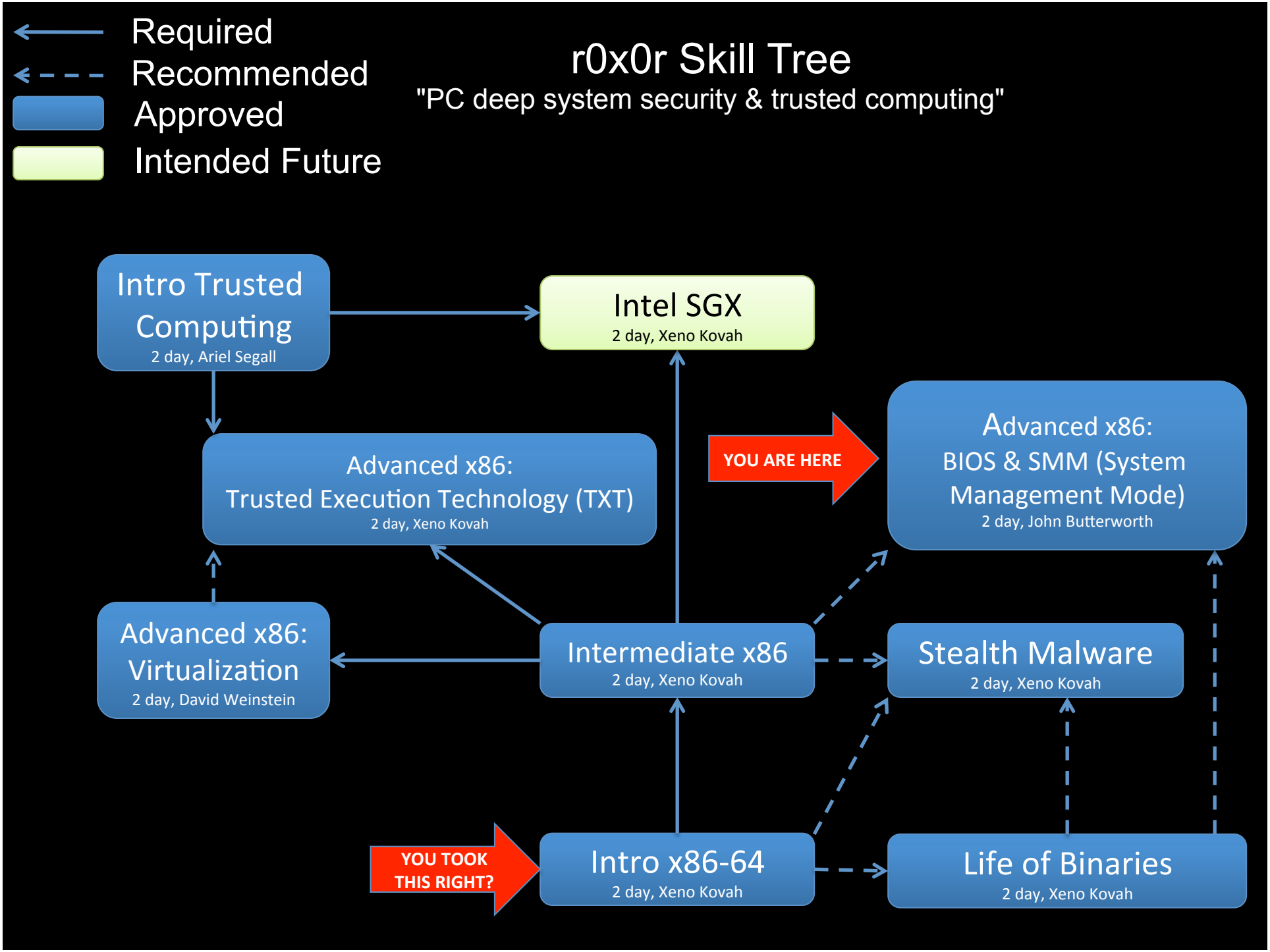
Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

Attribution condition: You must indicate that derivative work
"Is derived from Xeno Kovah & John Butterworth's ’Advanced Intel x86: BIOS and System Management Mode Internals"

Welcome x86 Machine Masters!!!

US VS THEM!

"With great power loader suit, comes great responsibility"


Required
Recommended
Approved
Intended Future
r0x0r Skill Tree
"PC deep system security & trusted computing"
Intro Trusted Computing
2 day, Ariel Segall
Intel SGX
2 day, Xeno Kovah
Advanced x86: Trusted Execution Technology (TXT)
2 day, Xeno Kovah
YOU ARE HERE
Advanced x86: BIOS & SMM (System Management Mode)
2 day, John Butterworth
Advanced x86: Virtualization
2 day, David Weinstein
Intermediate x86
2 day, Xeno Kovah
Stealth Malware
2 day, Xeno Kovah
YOU TOOK THIS RIGHT?
Intro x86-64
2 day, Xeno Kovah
Life of Binaries
2 day, Xeno Kovah

About Us

- We do digital voodoo :)
- Full time security researchers at MITRE since 2007
- Leading and working on our own research ideas since 2009
  - Basically a bunch of people propose ideas, some get selected, and they get funded from overhead money (i.e. not paid for or directed by government funds)
- Started out working on trustworthy Windows kernel rootkit detection via memory integrity checking & timing-based attestation (“Checkmate”)
- Eventually got interested in BIOS/SMM level threats, and started working on them in earnest around 2011
  - By 2012, had our first custom extra-security BIOS based on our previous work
  - By 2013, had our first BIOS exploit and a BIOS vulnerability/integrity checker (Copernicus)
  - By 2014, had *lots* of BIOS exploits and a slightly more trustworthy Copernicus 2
- Formed the LegbaCore security consultancy in Jan. 2015
- Continue to specialize in low level security, from the Windows kernel and lower

About Us

- Conferences, we've spoke at a few:
- BlackHat USA 2013-2015, BlackHat EUR 2014, IEEE S&P 2012, ACM CCS 2013, Defcon 2012 & 2014-2015, CanSecWest 2014-2015, PacSec 2013, Hack in the Box KUL 2013-2014, Hack in the Box AMS 2014-2015, Microsoft BlueHat 2014, Syscan 2013, EkoParty 2013, BreakPoint & RuxCon 2013-2014, Shmoocon 2012, 2014-2015, Hack.lu 2013-2014, NoSuchCon 2013, SummerCon 2014, ToorCon 2013, DeepSec 2014, VirusBulletin 2014, MIRCon 2014, AusCERT 2014, Trusted Infrastructure Workshop 2013, NIST NICE Workshop 2013, DOD Information Assurance Symposium 2013, and MTEM 2013

About You

- What is your name?

(What do you want/hope to get out of the class?)

- Did you watch any of the prerequisite classes? :P
  - Do you know C?
- What is your typical day-to-day job?

Course Goals

- Provide you a basic background in BIOS technologies
  - Very few people know anything about it. Knowledge is power :)
- Convince you that having unlocked BIOS is a really bad thing that can adversely affect the entire system during runtime
- Show you how to measure and interpret the results to understand if and how a system BIOS may be vulnerable
  - Provide you a lot of hands-on examples when possible so you can “see” the effects
  - Its such an abstract topic that provides very little visibility, I have sought to lift this veil
- Convince you that this problem IS solvable! Especially the information which we cover over these 2 days
- Introduce you to some forensics tools that can not only help you analyze and interpret whether a system BIOS is vulnerable, but also introduce you to some methods to analyze changes if you think a BIOS has been compromised
  - There is still a lot of work to be done on the latter

Course Outline Day 1

- BIOS Introduction
- Chipset basics
  - How to identify a chipset
- Boot process Overview
- Reset vector & BIOS Operating Environment
- PCI
  - PCI Option ROM attacks
- System Management Mode (SMM)
  - SMM attacks

Course Outline Day 2

- BIOS flash (Serial Peripheral Interface (SPI) mostly)
- Flash chip access control vulnerabilities
- Introduction to UEFI
  - Secure Boot & Measured Boot
  - Forensic analysis of UEFI BIOS
  - Reverse engineering BIOS files
- Trusted Computing technologies to try and detect BIOS attackers