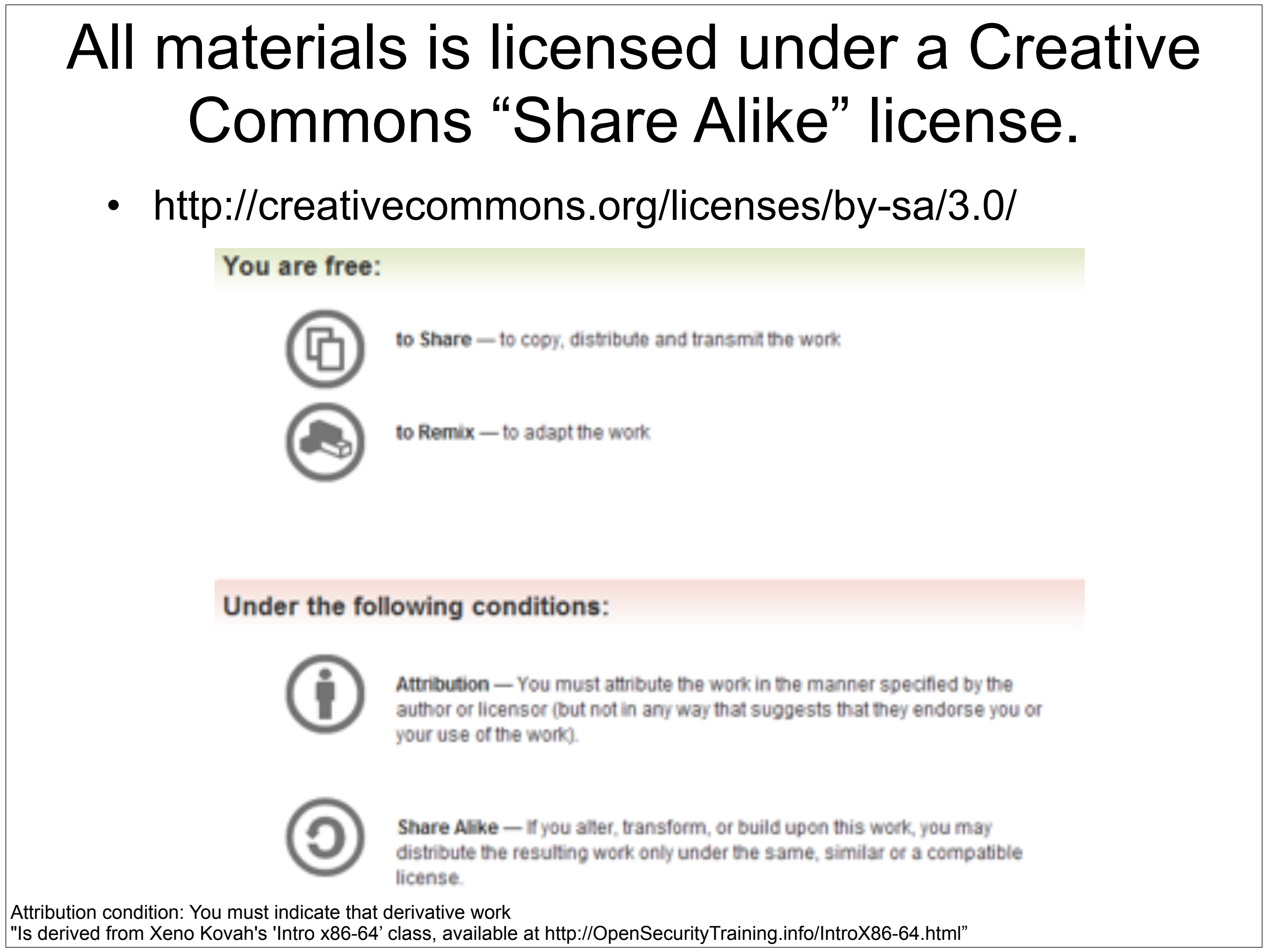
Introduction to Intel x86-64 Assembly, Architecture, Applications, & Alliteration

Xeno Kovah – 2014

xkovah at gmail



Attribution condition: You must indicate that derivative work

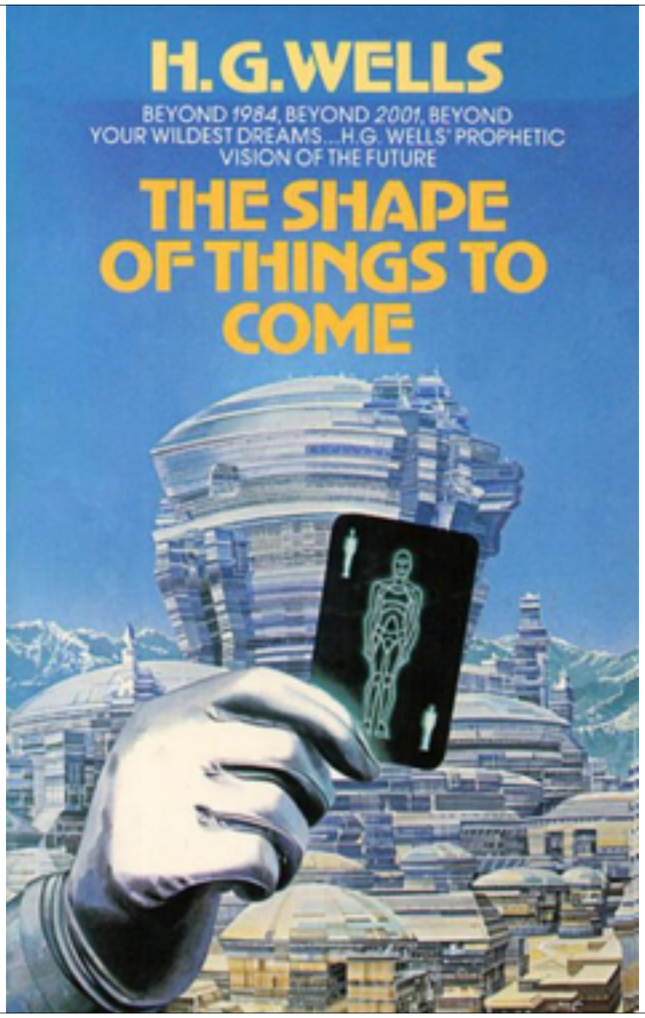
"Is derived from Xeno Kovah's ‘Intro x86-64’ class, available at http://OpenSecurityTraining.info/IntroX86-64.html"

Wrap up - instructions

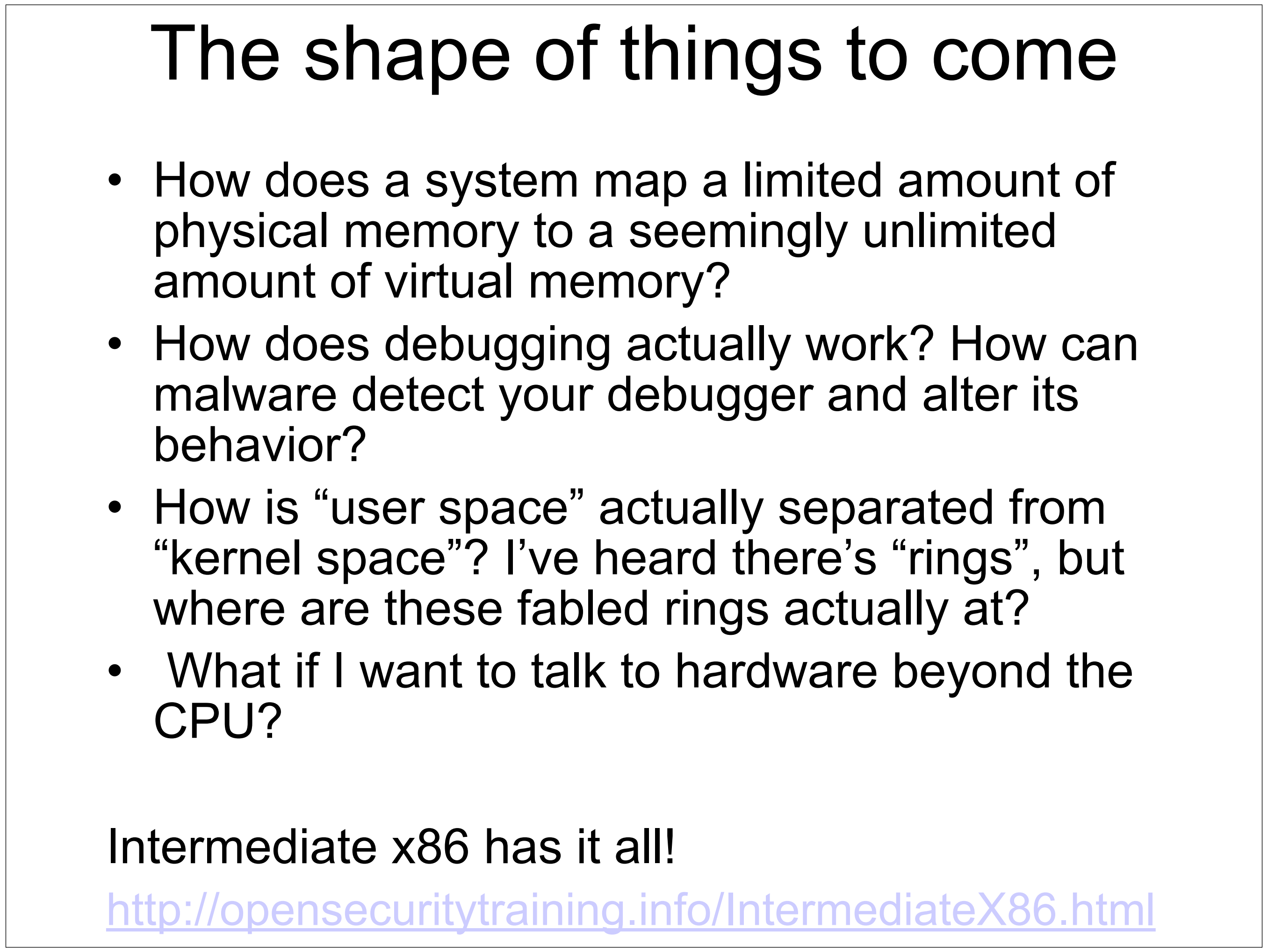
- Learned around 30 instructions and variations
- About half are just math or logic operations
- NOP
- PUSH/POP
- CALL/RET
- MOV/MOVZX/MOVSX/LEA
- ADD/SUB
- IMUL/DIV/IDIV
- JMP/Jcc (family)
- CMP/TEST
- AND/OR/XOR/NOT
- INC/DEC
- SHR/SHL/SAR/SAL
- REP STOS/REP MOVS

Wrap up

- Learned about the basic hardware registers and how they're used
- Learned about how the stack is used
- Saw how C code translates to assembly
- Learned basic usage of compilers, disassemblers, and debuggers so that assembly can easily be explored
- Learned about Intel vs AT&T asm syntax
- Learned how to RTFM
- Learned that classes that claim to teach you hacking/RE in a couple days are selling the *illusion* of understanding. An illusion which soon fades.


H.G.WELLS
BEYOND *1984*, BEYOND *2001*, BEYOND YOUR WILDEST DREAMS...H.G. WELLS' PROPHETIC VISION OF THE FUTURE
THE SHAPE OF THINGS TO COME

http://www.geofftaylor-artist.com/system/files/imagecache/normal/covers/wells_hg-shape_of_things_to_come.jpg



The shape of things to come

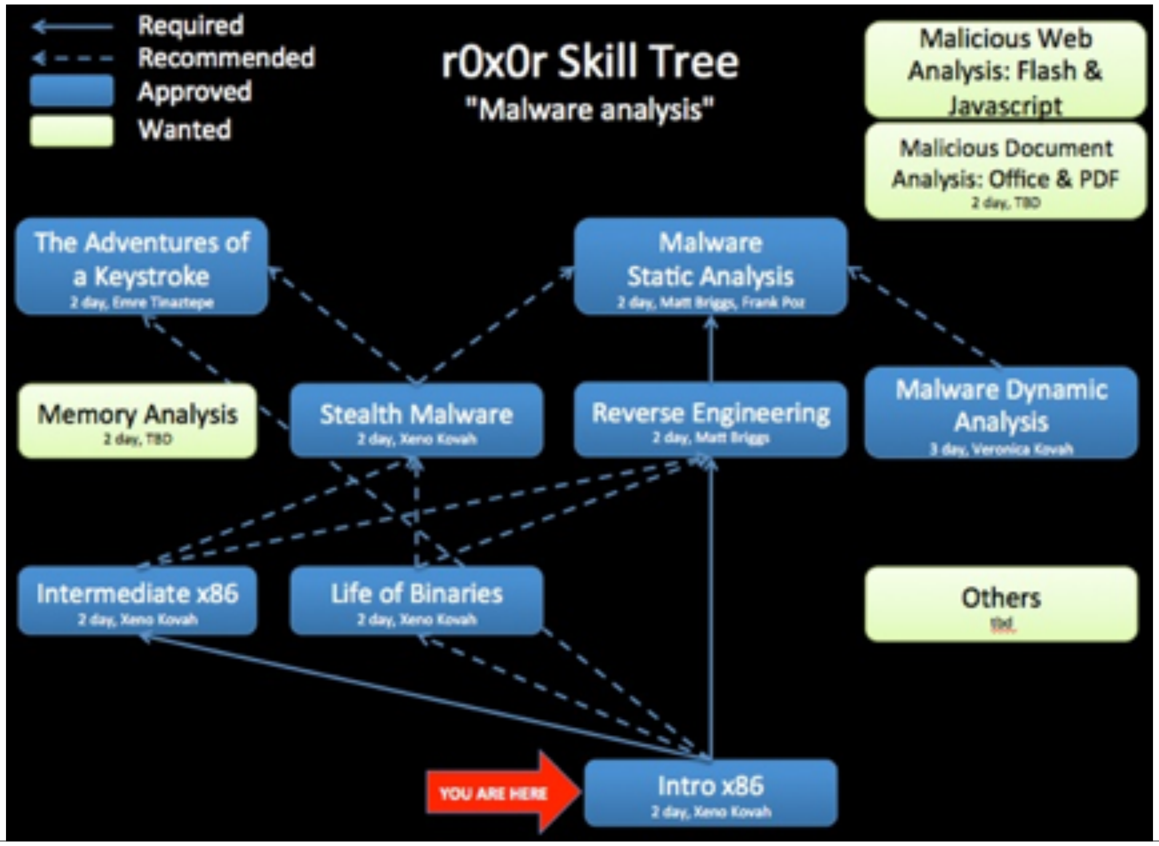
- How does a system map a limited amount of physical memory to a seemingly unlimited amount of virtual memory?
- How does debugging actually work? How can malware detect your debugger and alter its behavior?
- How is “user space” actually separated from “kernel space”? I’ve heard there’s “rings”, but where are these fabled rings actually at?
- What if I want to talk to hardware beyond the CPU?

Intermediate x86 has it all!

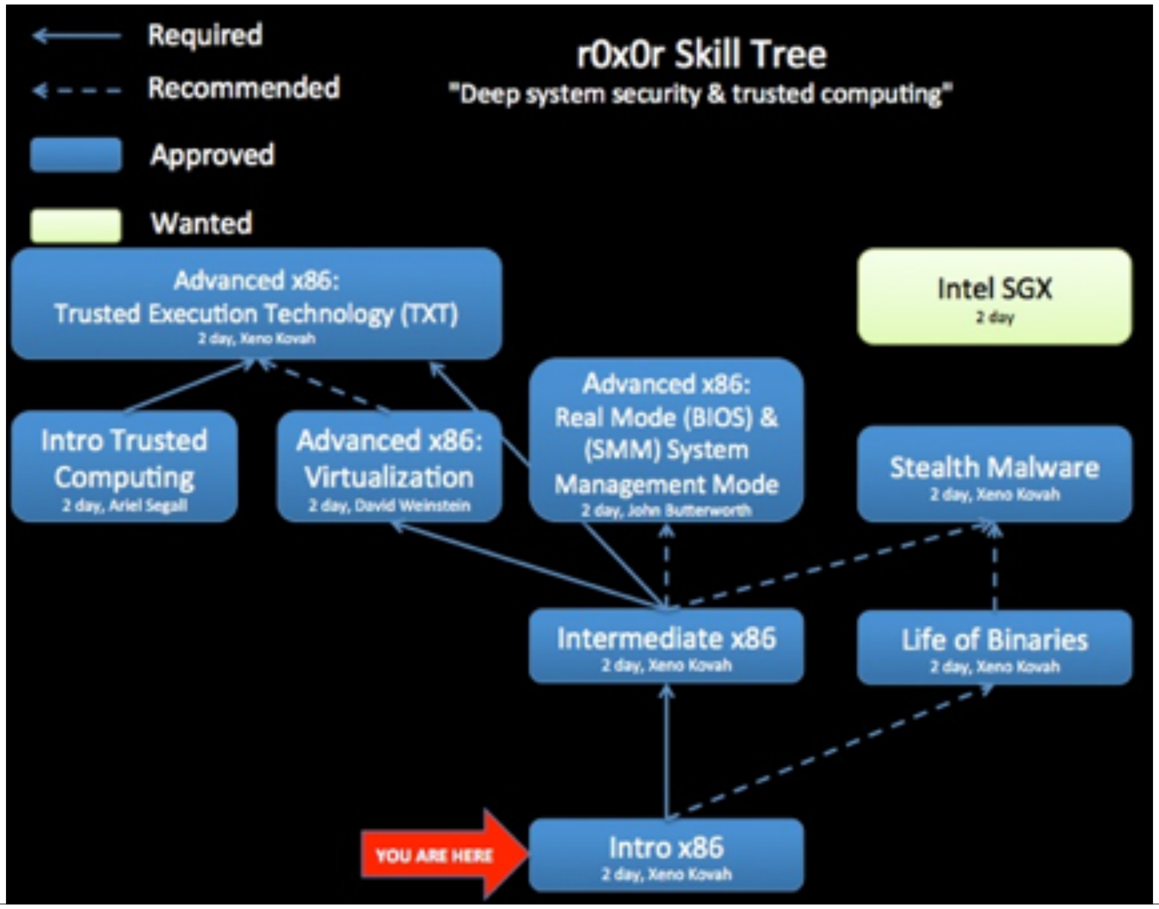
http://opensecuritytraining.info/IntermediateX86.html

http://www.geofftaylor-artist.com/system/files/imagecache/normal/covers/wells_hg-shape_of_things_to_come.jpg

Keep skilling up! Climb the r0x0r skill tree!
Take this class and teach others!
Contribute a new class in your expertise area!

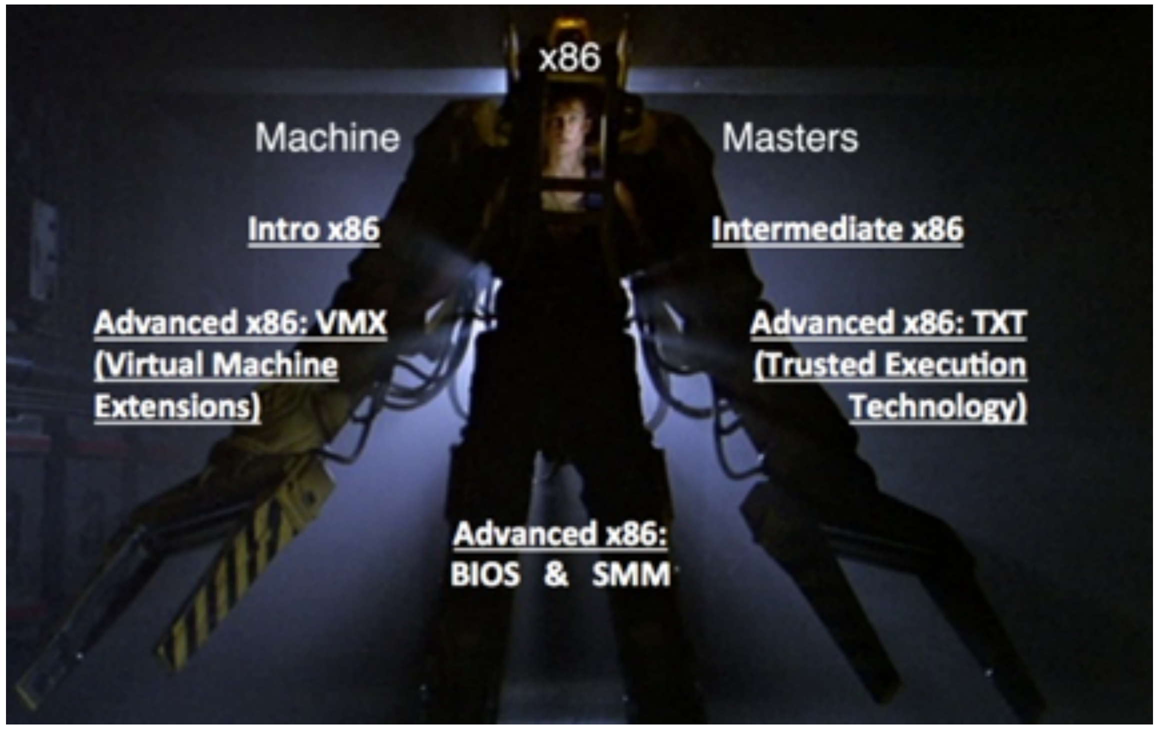


Use these skills towards the hardest game in town: defense!
Learn what trusted computing technologies can (and can't) offer!



Required
Recommended
Approved
Wanted
r0x0r Skill Tree
"Deep system security & trusted computing"
Advanced x86: Trusted Execution Technology (TXT) 2 day, Xeno Kovah
Intel SGX 2 day
Intro Trusted Computing 2 day, Ariel Segall
Advanced x86: Virtualization 2 day, David Weinstein
Advanced x86: Real Mode (BIOS) & (SMM) System Management Mode 2 day, John Butterworth
Stealth Malware 2 day, Xeno Kovah
Intermediate x86 2 day, Xeno Kovah
Life of Binaries 2 day, Xeno Kovah
YOU ARE HERE
Intro x86 2 day, Xeno Kovah

Or suit up just because it's the *hardcore* thing to do!


x86
Machine
Masters
Intro x86
Intermediate x86
Advanced x86: VMX (Virtual Machine Extensions)
Advanced x86: TXT (Trusted Execution Technology)
Advanced x86: BIOS & SMM

That's all Folks!