Scott Christensen
11/18/16
C.S. 465

Homework #13: Ken Thompson Compiler Hack

1) Describe briefly and clearly how the attack works

The goal of the attack is to produce 2 “Trojan horse’ self-reproducing programs into someone’s C compiler. To do this, it makes the compiler accept these Trojan horses by changing them into legal C binary code when the system recompiles. That way, the login command will remain bugger with no trace of change in source anywhere.

2) If you suspect that your machine has been compromised, what should you do about it?

Ken Thompson suggests that when considering such an attack as he has described, you should check for malicious code placed in your compiler. In general, one should use reliable backups for your information, change your passwords, install legitimate anti-virus protection, re-install your OS, etc.

3) What other kinds of software like compilers do we usually trust that have the potential to be compromised?

Other such soft that can ware can include (but is not limited to) most any program-handling program like ones assembler, loader, or even ones hardware microcode.