Christopher Morgan
CS 465
November 26, 2013

Homework 13

Read the classic Ken Thompson Compiler Hack article.

Answer the following questions:

1) Describe briefly and clearly how the attack works

The 'login' hack described in the article works by changing the definition of a compiler to accept a predefined password for any login. However, this attack is performed with a little bit more faness. The way the author describes this attack is the attacker first modifies the source of a compiler. The compiler in this case was modified so that whenever it sees the pattern of a UNIX login it would compile the login but also compile in a universal password as well. The attack continued by also inserting self-inserting code. In other words, once the evil compiler was compiled to evil binary the evil parts of the code could be removed and the evil binary would from then on reinsert itself whenever it was compiled. This allows the login command to remain bugged with no trace in the source code anywhere.

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

I'm not sure. I would guess that if one works for a company one could talk with the security team in your company. One could reinstall software and hardware from a trusted source. In the end however, the article make an interesting point, that one really can only trust what one dose or builds. Therefore, his point is write it or build it yourself, else in the end we're really just reliant on the trust of others. For example, if I don't trust any hardware company currently in the market, there isn't much I can do about it, given that I can make my own hardware.

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

The article makes the point that any software handling software that we use is vulnerable to this type of attack. I think of the python and java interpreters. I also think of assemblers, loaders, and hardware microcode. All of these could have similar vulnerabilities.