6.033 Computer System Engineering

Spring 2009

Preparation for Recitation 24

Read *Reflections on Trusting Trust*. This is one of our shortest readings--only three pages--but do not be deceived by its brevity. It is surprisingly deep and requires a lot of thinking to get your head around, but once you figure it out it is fascinating. Plus, you will know something that most people who haven't read this paper are quite clueless about.

This paper is probably best ingested by reading it carefully (your first reaction may be "What was that all about?"), discussing it in a small group, and then going back to read it again. Then discuss it in recitation, then read it a third time. On one of those three readings, you will probably say to yourself "Oh, now I get it!"

The paper emphasizes how difficult it is to be sure that you know what your software actually does. One way to avoid treacherous software would be to write all your software yourself. Although this approach would in principle solve the problem, it is overwhelmingly impractical. One has no choice but to rely on, and thus trust, software from other sources.

The paper has enough to think about while you are reading it. But here are some questions to think about later:

Two programmers, Alice and Bob, want to buy the latest version of the Microsoft C compiler. Alice searches the Internet for the lowest price and downloads the compiler from a web site on some island in the Pacific Ocean. Bob buys a CD that claims to contain the same compiler from the local computer store.

1. Who and what must Alice trust to believe that she received a compiler without Trojan horses?
2. How about Bob?

Since publication of Thompson's paper, there have been two proposals for handling trust in programs that you didn't personally write:

1. have the author sign the binary, using the techniques of chapter 11 of the 6.033 textbook, and
2. apply the methods of chapter 5 to run the program in a completely isolated environment, called a "sandbox".

Do these proposals solve the problem that Thompson raises? How do these proposals relate to the challenges that Alice and Bob face?