[CPSC 539B] HW5

Proof Carrying Code (PCC)

March 13, 2019

1 Critique

PCC is a technique that is used for safe execution of untrusted code. This approach is quite different from F to TAL. This is very similar to how formal verification works. The PCC consists of two parts the agent (code producer) and the host-system (code consumer). In PCC, the code producer or the agent creates a formal safety proof for the untrusted code with respect to the safety policies. The host system uses a proof validator to check that the proof is valid and can safely execute the untrusted code.

The Verification generator uses Floyd-style VC with VC (program, invariants, post-conditions) is interesting. Since they are encoding the proof in code, if the code-size is huge, it will be a problem. Annotations can be very painful, its still a problem. They claim that this is better than the cryptographic protocols because in that case we are trusting the authority, however, what about hash values? But since this paper came in 1996, I am assuming hash values were not a thing then. Hash values can't verify the correctness of the data, but can verify the integrity of the data. So maybe this is a different comparison altogether.

2 Open Questions

1. This is an entirely different approach from how a compiler works, right? The task of the compiler is to convert one language to another with correctness and safety properties so that the code can be executed. The goal of a PCC is two fold :
   (a) safe execution of untrusted code
   (b) linking different language codes based on this proof verification, right?