Question
Proof Carrying Code
March 24, 2005

Trust

1. It seems that PCC is really just integrating formal mathematical proof alongside the code for execution. While makes it possible for a machine to know to what degree it can trust a piece of code? (Darrell Hyatt)

2. Why the consumer should trust the safety proof no matter how the proofs are constructed? (Muhammad Abu-Saqer)

3. Why we can trust the checker or policy? (Muhammad Abu-Saqer)

Security

4. PCC provides a way to verify a program's safety based on a "safety policy", but is there any way to verify that the safety policy covers all of the possible vulnerabilities? (Sean Kugele)

5. In the paper from last lecture on "Flexible Containment" if a policy did not explicitly grant a privilege it was implicitly denied, which seems like a sensible design decision. In PCC, the nature of the system seems to be that if a privilege is not explicitly denied then it is implicitly allowed. Is this correct? (Sean Kugele)

6. The authors state that VCGen relies on the code annotations from a potentially untrustworthy code producer, later stating that VCGen "must be careful not to allow incorrect annotations to hide unsafe program behavior"; however I do not remember them mentioning how this is done. Was this stated somewhere in the paper? It seems that in order to verify that a code annotation is valid VCGen would need to infer the behavior of the actual code, which would defeat the purpose of the annotation. (Sean Kugele)

7. They aren't very concerned with code and proofs that are modified yet still pass verification, saying that passing verification means the new code is safe. Why is this the case? (Lee Smith)

8. Could the code produce fake the safety proof? if yes how the code consumer identify the correct proof from the fake one? (Muhammad Abu-Saqer)

9. Does PCC check against the access control? (Muhammad Abu-Saqer)

10. How can we make sure the rules we make are correct? (Muhammad Abu-Saqer)

11. The safety policy is the key part for proof-carrying code security. In the author’s experiment, the safety rules are specified using first-order logic, which involves understanding of the
semantics and syntaxes of the rules. In practice, what is the difficult level of the implementation of the safety policy? (Haiyan Cheng)

12. The author mentioned that one of the advantages of proof carrying code is that it used static checking instead of the dynamic checking, what is the disadvantages of the static checking? (Haiyan Cheng)

13. Is safety policy a subset of security policy? Is it possible that the Proof Carrying Code technology be extended to include specifying the security policy? (Haiyan Cheng)

14. In order to check the proof, does the code consumer require additional information from the code producer? Such as type and dataflow information. (Haiyan Cheng)

**Implementation**

15. The authors say that "relying on the correctness of a complex theorem prover" is dangerous, but what keeps the VCGen from becoming more complex over time anyway? (Darrell Hyatt)

16. Are new proofs needed every-time a piece of code is changed? how does the amount of change in code effect the generation of the proof? (Ranjit Randhawa)

17. Are there languages that you cannot port PCC to? (Ranjit Randhawa)

18. PCC are similar to the compiler static type checking, does this mean that PCC could provide flexibility in proof checking at run-time. is this one of tradeoff of the PCC. (Muhammad Abu-Saquer)

19. Compare and contrast PCC with other kinds of protection against untrusted code like hardware isolation (where you load each untrusted code in its own address space. Then disallow memory access or jump to any address outside the allocated space) and sandboxing. (Muhammad Abu-Saquer)

20. Does the code consumer’s safety policy language depend on the system used? (Haiyan Cheng)

21. Could the size of proof affect the performance? (Muhammad Abu-Saquer)

22. One of the reasons Java programs run slowly is because of the overhead associated with run-time checking. Could the PCC used to eliminate some of these run-time checking? (Muhammad Abu-Saquer)