Reading Questions 5 (optional)

CMU 17-654/17-754: Analysis of Software Artifacts
Jonathan Aldrich (`jonathan.aldrich@cs.cmu.edu`)

Due: Tuesday, April 19, 2005 (10:30 am)

10 points total

Readings:

- Oleg Sheyner and Jeannette Wing. Tools for Generating and Analyzing Attack Graphs. Formal Methods for Components and Objects, 2004.
- David Brumley and Dawn Song. Privtrans: Automatically Partitioning Programs for Privilege Separation.
- David Brumley and Dan Boneh. Remote Timing Attacks are Practical.

Questions:

- At the end of section 4, Sheyner et al. suggest that actions like applying system patches can be used to reduce the attack graph until there are no possible attacks. Does this suggest that attack graphs are not useful if you have applied all security patches to a system? Why or why not?
- Security analyses like the tainted analysis you have implemented improve security by finding and eliminating explicit security holes. A skeptic asks, since the Privtrans system does not help users in finding errors such as buffer overflows, what good could it possibly do to help security? How would you answer the skeptic?