6.033 Computer System Engineering
Spring 2009

Preparation for Recitation 21

For today, read Jonathan Pincus and Brandon Baker, *Beyond Stack Smashing: Recent Advances in Exploiting Buffer Overruns*.

Stack smashing is one of the most frequent attacks used on computer systems that run software written in the C programming language. Most simple attacks won't work anymore, but attackers have come up with more sophisticated versions. This paper describes some of those versions. As you read this paper, you may ask yourself what is the root problem that allows stack smashing?