0. Introduction

There are many ways to attack computers. Today we study one of the "classic" methods.

As mentioned in the reading, hackers have adapted this method to different attacks. All of these attacks derive from the "classic" buffer overflow.

We study this attack not to teach you all to become hackers but rather to educate about vulnerabilities: what they are, how they work, and how to defend against them. Please remember: _although the approaches used to break into computers are intellectually very interesting, breaking in to a computer that you do not own is, in most cases, a criminal act_.

1. Let’s examine a vulnerable server

2. Let’s examine how an unscrupulous element (a hacker, a script kiddie, a worm, etc.) might exploit the server.

3. What is the root cause of such vulnerabilities? What if the server were written in Java?

4. How have attackers moved beyond the classic attack, and why have they had to do so?

Thanks to Russ Cox for the code and various pointers.