

Handout 3 (Buffer Overflow Attacks)

By far the most popular attack method on computers are buffer overflow attacks or variations thereof. The popularity is unfortunate because we now have technology to prevent them effectively. But these kind of attacks are still very relevant even today since there are many legacy systems out there and also many modern embedded systems do not take any precautions to prevent such attacks.

To understand how buffer overflow attacks work we have to have a look at how computers work “under the hood” (on the machine level) and also understand some aspects of the C/C++ programming language. This might not be everyday fare for computer science students, but who said that criminal hackers restrict themselves to everyday fare? Not to mention the free-riding script-kiddies who use this technology without knowing what are the underlying ideas.

For buffer overflow attacks to work a number of innocent design decisions, which are benign on their own, need to conspire against you. One such design decision is how the memory is laid out for each process.

If you want to know more about buffer overflow attacks, the original Phrack article “Smashing The Stack For Fun And Profit” by Elias Levy (also known as Aleph One) is an engaging read:

<http://phrack.org/issues/49/14.html>