Week 1

Help

Memory-based attacks

We will begin our discussion of software security by understanding one of the oldest and pernicious attacks against software: the *buffer overflow*. We will see how buffer overflows are one kind of memory-based attack that low-level software (written in C and C++ primarily) is susceptible to, and we will consider other memory-based attacks as well. Your project for this week will be to construct a simple exploit of a buffer overflow, to see how it works.

If you have not done so, please watch the preparatory material from Week 0.

Learning Objectives

After the completion of this week's material (including the project, due at the end of next week), you will be able to:

- Understand the standard memory layout of running processes on the x86 architecture
- Identify buffer overflows and related memory-based vulnerabilities in C programs, such as those based on format strings
- Construct a simple exploit of a buffer overflow
- Understand how exploits can inject remote code, and perform other security compromises

Video Lectures

- Low-Level Security: Introduction (6:20)
- Memory Layout (10:57)
- Buffer Overflow (6:10)
- Code Injection (6:33)
- Other Memory Exploits (11:52)
- Format String Vulnerabilities (6:43)

Readings

Required reading

The only required reading this week is the following:

- Common vulnerabilities guide for C programmers. Take note of the unsafe C library functions listed here, and how they are the source of buffer overflow vulnerabilities. This list will be relevant for the project and this week's quiz.
- (Reference) Memory layout. Explains a C program's memory layout, replicating the discussion in the second lecture.

Supplemental readings

The following readings are optional: They are meant to supplement the material you are getting in the videos. Check them out if you are interested in learning more, or if you just want to see it all explained in a different way.

- Smashing the Stack for Fun and Profit - original article on the topic by Aleph One, in 1996
- Exploiting Format String Vulnerabilities - report describing these format string attacks when they were first recognized
- Basic Integer Overflows - discussion of how overflowing integers can be a vector of attack

---

Project

The first project is on exploiting buffer overflows; it is **due in two weeks**, just prior to the start of week 3. You will complete the work for the project on your own computer, and then take the on-line assessment to show that you've done so.

Quiz

The quiz for this week covers all of the material for this week, *and the introductory material from last week*, so do not forget to view that too. You must submit the quiz no later than the start of week 2. You will have three attempts to complete the quiz, at two hours per attempt. It consists of 15 questions, and if you are well versed in the material it should take about 30 minutes (but longer if you have to go back and look things up, obviously).

Created Wed 9 Apr 2014 6:15 AM PDT

Last Modified Sun 2 Nov 2014 4:44 AM PST