98-212: Competitive Computer Security

Instructor: Maxime Serrano (mserrano@cmu.edu)

Fall 2013

Welcome to 98-212, Competitive Computer Security!

This is a technical course focused on offensive computer security, particularly in the context of the computer security competitions called "Capture the Flag" competitions. Its primary purpose is to teach the tools and tricks used in offensive security, both for the purpose of honing your skills for these competitions and also for use in better understanding what an attacker might actually be capable of.

My name is Maxime Serrano - I am a Junior in Computer Science and Mathematical Sciences, and the leader of the "Plaid Parliament of Pwning" - which we usually refer to as the slightly-less-ridiculous "PPP." PPP is Carnegie Mellon's CTF team, as well as a security research group. It is sponsored by professor David Brumley from the ECE department (who teaches the fantastic 18-487 course). PPP is ranked as one of the best teams in the world, consistently taking home first place finishes, most recently at DEFCON in Las Vegas and SECUINSIDE in Seoul, South Korea. In fact a global ranking of CTF teams recently ranked PPP as the best team in the world, and as the only American team in the top 10.

CTFs are competitions held both online and in-person at conferences that are competed in by many people active in information security. Many companies send unofficial teams - for example, Raytheon SI, ManTech and Google are represented. A few universities also have teams, such as CMU, UC Berkeley, UC Santa Barbara, Georgia Tech, Boston University, and RPI.

This course will be held on Thursdays from 6:30 to 8 pm in Wean Hall 5403. We will cover topics ranging throughout many aspects of computer security, including forensics, web security, cryptography, reverse engineering and binary exploitation.

1 Course Policies

The StuCo system requires that I take attendance, so I will. You are allowed 2 unexcused absences, as well as arbitrarily many "excused absences." There are two primary ways to be excused. First, you can have an actual emergency - in which case just toss me an email and everything will be fine. Second, you can complete the "homework" that is posted for that week. The homework *will be hard* if you do not come to lecture, and will be *easy* - but still worth doing, if you're interested - if you do.

2 Rough Schedule

The plan is currently to follow roughly the following order:

1. September 5: Data encodings and steganography.
2. September 12: Disk and network forensics.
3. September 19: Classical cryptography.
4. September 26: Web security: XSS, CSRF.
5. October 3: Web security: SQL injection, command injection, misc.

6. October 10: x86 refresher, introduction to reverse-engineering.
7. October 17: Buffer overflows day one: zero protections.
8. October 24: Buffer overflows day two: NX & ASLR.
9. October 31: Modern cryptography day one: hashing & RSA.
10. November 7: Modern cryptography day two: side-channel attacks, CRIME.
11. November 14: Possibly no class
12. November 21: Exploitation day three: format strings.
13. December 5: TBA.