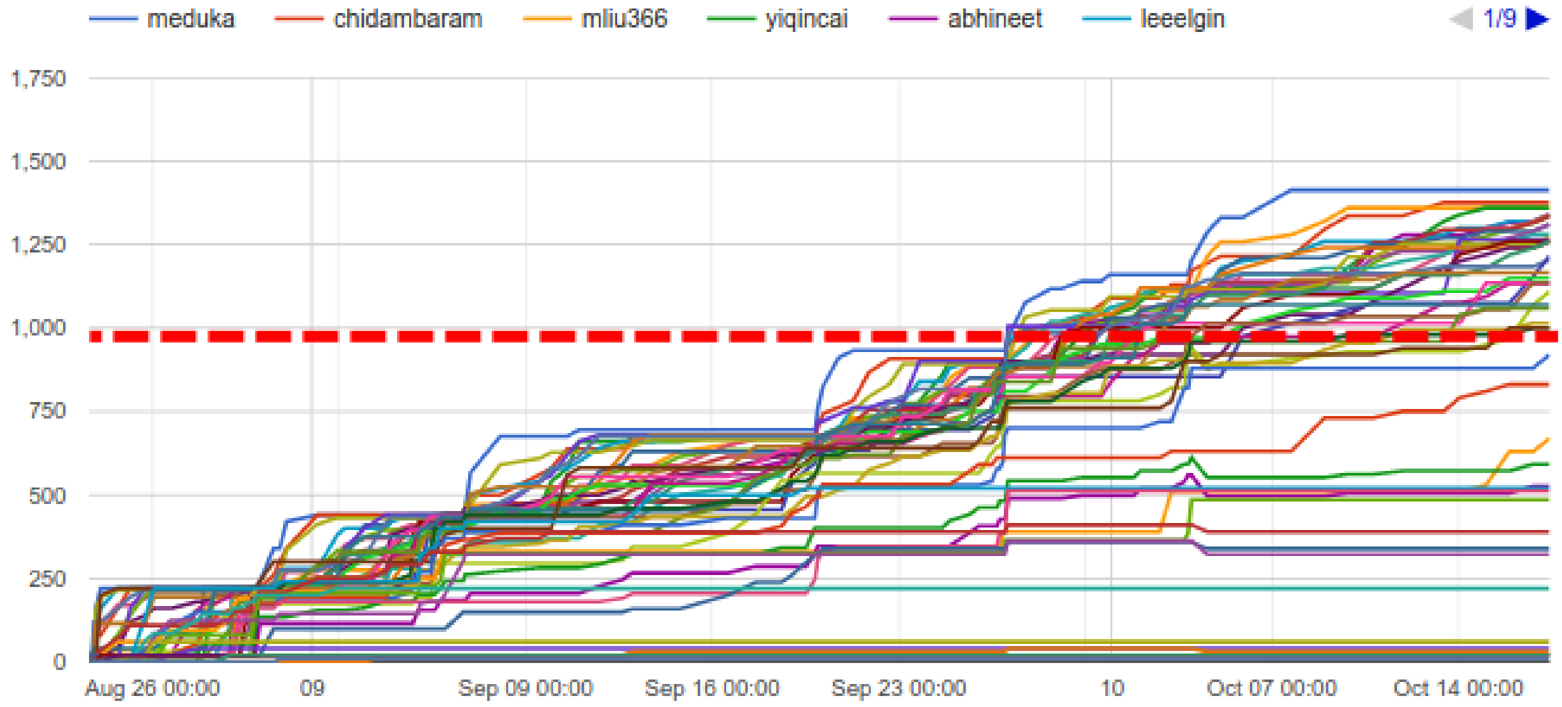
Lec09: Remote Exploit

Taesoo Kim

Scoreboard


meduka
chidambaram
mliu366
yiqincai
abhineet
leeelgin
1/9
1,750
1,500
1,250
1,000
750
500
250
0
Aug 26 00:00
09
Sep 09 00:00
Sep 16 00:00
Sep 23 00:00
10
Oct 07 00:00
Oct 14 00:00

Note on Score/Grade

- 160 per lab x 6 labs = 960 for A
- So far, except 4, all A
- If you want to get A, there are plenty of other options:
    - NSA Codebreaking challenges
    - Solving old labs/challenges (50% penalty)
    - Win TKCTF :)

Administrivia

- In-class CTF: https://ctf.gts3.org/ (Open to public!)
  - Registration: http://bit.ly/tkctf_register (**#2-4** persons per team)
  - Rules: https://tc.gts3.org/cs6265/2019/ctf.html
  - Submit your team's challenge by Nov 14
- Due: Lab07 is out and its due on Oct 31 (two weeks)!
- NSA Codebreaker Challenge → Due: Dec 06

Best Write-ups for Lab06

rop-basic	mliu366, dlaw6
rop-64	mliu366, viyer43
pop	viyer43, mliu366
puzzle	ochbaklo, Aditi
upto-retaddr	ochbaklo, meduka
find-gadget	achang66, Aditi
sprintf	chidambaram, yiqincai
rop-sorting	chidambaram, achang66
inc1	chidambaram, yiqincai
fmtstr-relro	chidambaram, leeelgin

Summary of Lab06 (1)

- DEP/ASLR are not perfect solutions (pretty good mitigation?)
  - DEP: ret-to-lib, ROP
  - ASLR: code leakage
- What about stack canary? (what if we placed it together?)
- Lots of known defenses (e.g., CFI)

Summary of Lab06 (2)

- Generic computation
    - puzzle: arbitrary string
    - rop-sorting: arbitrary computation
- ROP gadgets
    - pop: from an immediate operand
    - upto-retaddr: pivoting stack
    - find-gadget: even from compiler-supplied code
- Attack vector
    - fmtstr-relro (under RELO), sprintf, inc1

Remote Challenges

- Use techniques learned from Lab01-Lab06
- But targeting the remote server (e.g., online services)!

In-class Tutorial

- Step1: nc
- Step2: brute force attack
- Step3: guessing attack
- Step4: crackme0x00 in a remote setting (tut02)

```
$ ssh lab06@3.95.14.86
Password: <password>

$ cd tut07-socket
$ cd tut07-remote
```