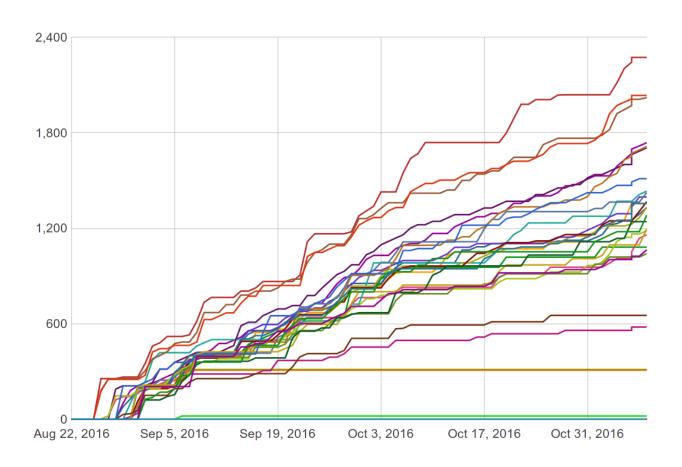
Lec10: Heap Exploitation

Taesoo Kim

Scoreboard



NSA Codebreaker Challenges

| University | Task 1 | Task 2 🔻 | Task 3 🔻 | Task 4 🔻 | Task 5 🔻 | Task 6 🔻 |
|---|--------|----------|----------|----------|----------|----------|
| Georgia Institute of Technology | 54 | 44 | 39 | 28 | 14 | 4 |
| Carnegie Mellon University | 28 | 26 | 16 | 11 | 5 | 2 |
| Dakota State University | 56 | 40 | 26 | 20 | 8 | 0 |
| New Mexico Institute of Mining & Technology | 13 | 13 | 12 | 11 | 6 | 0 |
| Naval Postgraduate School | 7 | 7 | 6 | 6 | 5 | 0 |
| University of Colorado at Colorado Springs | 14 | 12 | 9 | 9 | 3 | 0 |
| Davenport University | 9 | 8 | 7 | 6 | 3 | 0 |
| University of Maryland, Baltimore County | 26 | 22 | 13 | 11 | 2 | 0 |
| Arizona State University | 20 | 19 | 12 | 9 | 2 | 0 |
| University of Hawaii | 11 | 10 | 8 | 8 | 2 | 0 |
| Showing 1 to 10 of 385 entries | | Previous | 1 2 | 3 4 | 5 : | 39 Next |

Administrivia

- Just one more lab after this week!
- Last lab (Lab11) includes alternative Web exploitation (e.g., xss/sqlinj)
- Last lecture (Dec 2): real-world exploit (iPhone jailbreaking) + NSA Q&A
- Due: Lab10 is out and its due on Nov 17
- NSA Codebreaker Challenge → Due: Dec 1

Grading

- In the last lecture (Dec 2), we will let you know your grade
- If that's not the grade that you wanted, you have two more weeks for additional work (let's discuss in person)

Discussion: Lab09

- What's the most "annoying" bug or challenge?
- What's the most "interesting" bug or challenge?
- or .. just exhausted?

Discussion: snake

- What was the problem?
- How did you exploit?

Discussion: 2048-int

- What was the problem?
- How did you exploit?

Discussion: intq

- (in 64-bit) what does the expression, 1 > 0, evaluate to?
 - ? (a) == 0, (b) == 1, (c) == NaN, (d) == -1
- (unsigned short)1 > -1?
 - ? (a) == 1, (b) == 0, (c) == -1, (d) undefined
- -1U > 0?
 - ? (a) == 1, (b) == 0, (c) == -1, (d) undefined

Discussion: intq

- -1L > 1U? on x86-64 and x86
 - ? (a) 0 on both platforms, (b) 1 on both platforms, (c) 0 on x86-64, 1
 on x86, (d) 1 on x86-64, 0 on x86
- UINT MAX + 1?
 - ? (a) 0, (b) 1, (c) INT_MAX, (d) UINT_MAX, (e) undefined
- (in 32-bit) what's abs(-2147483648)?
 - ? (a) == 0, (b) < 0, (c) > 0, (d) == NaN

Discussion: intq

- -1 << 2?
 - ? (a) 0, (b) 4, (c) INT_MAX, (d) INT_MIN, (e) undefined
- INT_MAX + 1?
 - ? (a) 0, (b) 1, (c) INT_MAX, (d) UINT_MAX, (e) undefined
- -INT_MIN?
 - ? (a) 0, (b) 1, (c) INT_MAX, (d) UINT_MAX, (e) INT_MIN, (f) undefined

Discussion: race

- What was the problem?
- How did you exploit?

Discussion: urandom

- What was the problem?
- How did you exploit?

Discussion: tictou

- What was the problem?
- How did you exploit?

Discussion: django

- What was the problem?
- How did you exploit?

Discussion: type

- What was the problem?
- How did you exploit?

Discussion: fsb-heap2

- What was the problem?
- How did you exploit?

Lab10: Heap Exploitation

- various malloc implementation (e.g., dlmalloc, ptmalloc)
- use-after-free
- double-free techniques

Today's Tutorial

- In-class tutorial:
 - Your first heap exploitation
 - Exploring heap memory structure in G

In-class Tutorial

```
$ git git@clone tc.gtisc.gatech.edu:seclab-pub cs6265
or
$ git pull
$ cd cs6265/lab10
$ ./init.sh
$ cd tut
$ cat README
```