Lec00: Security Vulnerabilities and Their Mitigation in Native Code

Taesoo Kim

About Myself

- Educational Background
  - 2014-20??: Assistant Professor at Georgia Tech
  - 2009-2014: S.M./Ph.D. from MIT in CS
- Research interests:
  - Operating systems, Systesms security, Bug findings, etc.

Visit: https://taesoo.kim or https://gts3.org

SSLab: Systems Software and Security Lab

Research Interests

1. **Bug finding**:
    - e.g., static analysis, fuzzing, symbolic execution, etc.
2. **System security**:
    - e.g., system updates, Intel SGX, sandboxing, etc.
3. **System scalability**:
    - e.g., file system, graph processing, scalable lock, etc.

Research Contributions

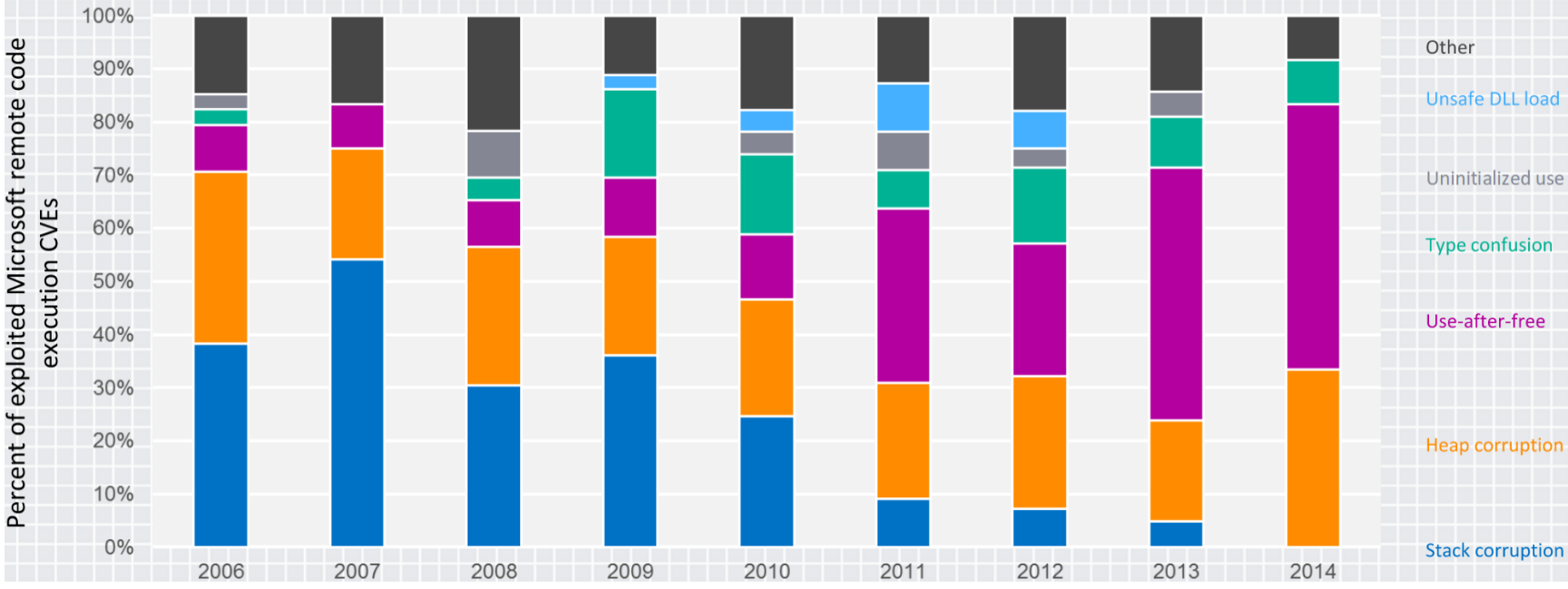
- Over 300 bug fixes and numerious CVEs in Linux, Firefox, OpenSLL, etc.

DEFKOR00T Won DEF CON CTF'18!

Today's Agenda

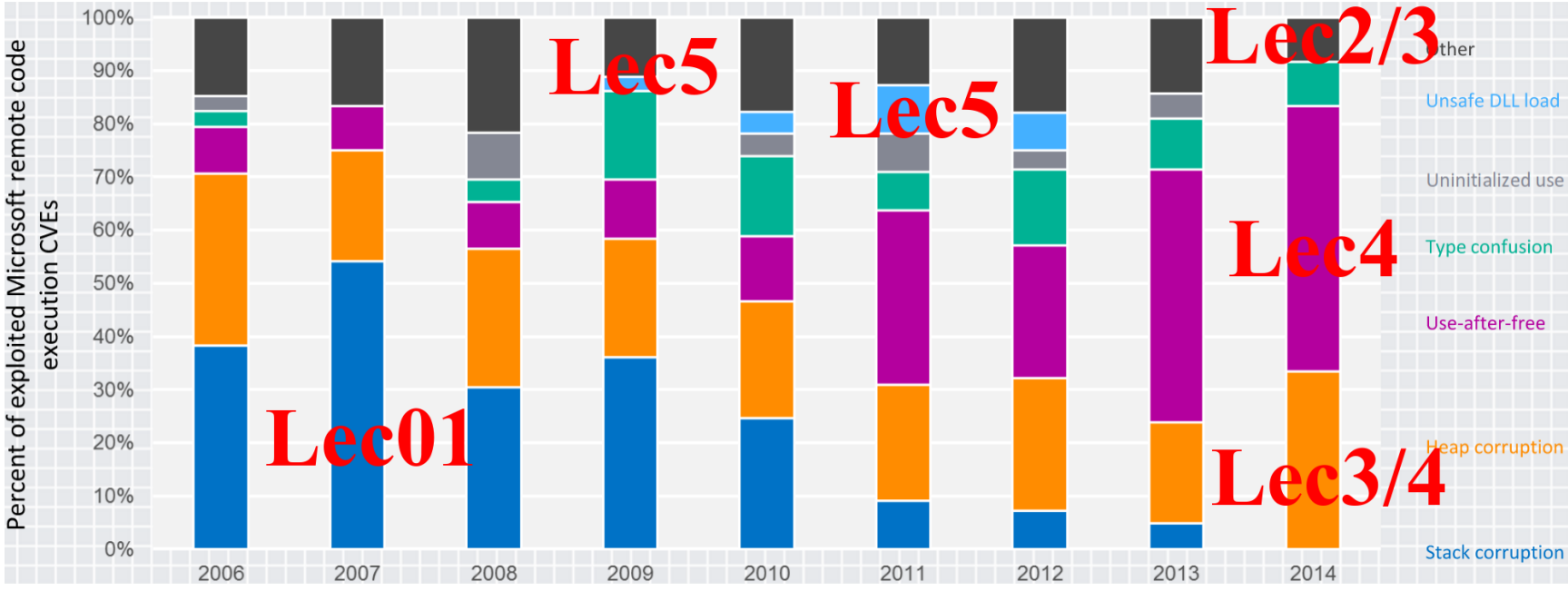
- 10:00-10:50: **Lec01**: Stack Overflow and Protections
- 11:00-11:50: **Lec02**: Format String Vulnerabilities
- *12:00-12:50: Lunch break*
- 01:00-01:50: **Lec03**: Integer Overflow and Undefined Behavior
- 02:00-02:50: **Lec04**: Heap-related Vulnerabilities
- 03:00-03:50: **Lec05**: Advanced Topics in Security
- 04:00-04:50: **Lec06**: **Tutorial** on Fuzzing and Sanitizers

Trends of Vulnerability Classes (by MS)



Ref. Exploitation Trends: From Potential Risk to Actual Risk, RSA 2015

Goal: Understanding Classes of Vulns.



Ref. Exploitation Trends: From Potential Risk to Actual Risk, RSA 2015

Using Recent/Real-world Examples

Lec01.
- Ex1. CVE-2017-15118: QEMU
- Ex2. CVE-2014-4975: Wireshark
- Ex3. CVE-2015-7547: glibc*

Lec02.
- Ex1. Linux block (CVE-2013-2851)
- Ex2. Linux ext3 (CVE-2013-1848)
- Ex3. sudo (CVE-2012-0809)

Lec03.
- Ex1. Android (CVE-2015-1538, CVE-2015-3824)
- Ex2. Linux Keyring (CVE-2016-0728)

Lec04.
- Ex1. OpenSSL (CVE-2014-0160)
- Ex2. Wireshark (CVE-2018-11360)
- Ex3. Linux vmcache (CVE-2018-17182)*

Lec05.
- Ex1. Linux Perf (CVE-2009-3234/+)
- Ex2. Linux USB (CVE-2016-4482)

Tutorial: Fuzzing and Sanitizers

```
# if you haven't downloaded yet!
$ wget https://www.dropbox.com/s/7nlsvkg68l70ez8/nutanix.tar.xz
  (or use: https://tc.gts3.org/public/tmp/1180f-nutanix.tar.xz)
$ unxz fuzzing.tar.xz
$ docker load -i fuzzing.tar
$ docker run --privileged -it fuzzing /bin/bash

# in docker
$ git pull
$ cat README
```