Mofassir Ul Haque Guest Lecture Summary

Josiah Craw
35046080

August 20, 2019

In this guest lecture we covered secure software, vulnerabilities, exploitation, and tools that are used within the industry. First, Mofassir discussed what a vulnerability is, they are usually a design flaw, an implementation bug or an improper implementation. Some examples of these are, the design of the internet, as a design flaw as it was designed before hacking of internet vulnerabilities was considered. This is an issue now as the internet has expanded and vulnerabilities are a key design consideration. The next example covered a implementation bug, this is when a programmer has a code based flaw that could be exploited. The final example is an improper configuration, this is when the software is designed well and there are few to no exploitable flaws however, the end user has set the software up poorly like leaving the password as the default.

Mofassir then covered exploitations, these are when a person of party find a vulnerability and exploit it some examples are given.

- Loss of sensitive information
  - Capital One Bank lost more than 100 million records
  - The European GDPR allows a fine for a loss equal to either 10 million Euro or 4% of a companies annual turnover
    - British Airways lost 500,000 records 200 million Euro fine
    - Marriot Hotel lost 3 million records and received a 110 million euro fine
- DDoS GitHub had 1.35 Terabits per second of traffic through a DDoS attack in the 1st quarter of 2019
- Firewalls, Anti-Virus, IDS, IPS are not particularly effective

The next component of the lecture was on the tools used by hackers and professionals as well as governments to access different software. Mofassir told us these can be broken down into three categories:

- Free tools
- Paid tools
- Custom tools, these are mostly used by governments