CS 458/658 - Computer Security and Privacy **Fall 2018**

Lecture 3: September 13, 2018

Lecturer: Ian Goldberg *Notes By: Harsh Mistry*

3.1 Program Security Continued

3.1.1 Intentional Malicious Flaws

3.1.1.1 Logic Bombs

- A logic bomb is malicious code hiding in the software already on your computer, waiting for a certain trigger to ”go off”
- Often placed by an insider and the trigger is often something the insider has influence over after leaving.

3.1.1.2 Spotting Trojan horses and logic bombs

- Spotting trojan horses and logic bombs is difficult because the end-user is intentionally running code.
- To avoid trojans you could not run untrusted code, but thats not always a guarantee.
- A better solution for avoiding malicious code is to prevent software from doing harmful things

3.1.2 Other Malicious Flaws

3.1.2.1 Web Bugs

- A web bug is a an object (usually a 1x1 pixel) embedded in a page which is fetched from a different server from the on that served the web page itself.
- Information about you can be sent to a third-party server which could be used in various ways such as tracking for advertisements
- Web bugs are considered malicious code because web bugs are an privacy more than security, as it violates the concept of *informational self-determination*

3.1.2.2 Back Doors

- A back door is a set of instruction designed to bypass the normal authentication mechanism and allow access to the system

3.1.2.3 Salami Attacks

- A salami attack is an attack that is made up of many smaller, often considered inconsequential
- A classic example would be, stealing fraction of cents of round-off from many accounts.

3.1.2.4 Privilege Escalation

A privilege escalation is an attack which raises the privilege level of the attacker (beyond that to which he would ordinarily be entitled)

3.1.2.5 Rootkits

- A rootkit is a tool often used by *script kiddies*
- It has two main parts
  - A method for gaining unauthorized root privileges.
  - A way to hide its own existence, so the root kit can't be detecting

3.1.3 Non Malicious Flaws

3.1.4 Covert Channels

- An attacker creates a capability to transfer sensitive/unauthorized information through a channel that is not supposed to transmit that information