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 Unintentional Flaws Continued

3.1.1.1 TOCTOU Errors

- Time of Check to Time of Use errors or otherwise known as race-conditions are errors caused by a change of state after a verification check
- The fundamental problem is the after a verification is done, certain values can be modified to allow for access to disallowed behaviour.
- Defences
  - When performing a privileged action on behalf of anoteh rparty, make sure all information is constant
  - Keep a private copy of request, so it can't be altered.
  - Where possible act on the object itself, and not on some level of indirection
  - If above cases do not apply, use locks to ensure the object is not changed during run time

3.1.2 Intentional Malicious Flaws

Various forms of software are written with malicious intent, but a common characteristic is all malware needs to be executed in order to cause harm. The types of malware are Viruses, Worms, Trojans, and Logic Bombs

3.1.2.1 Viruses

- A virus is malware that infects other files in attempt to replicate it self.
- Viruses typically exuctables are modified to include jump instructions to the virus code in effort to ensure the virus propagates across the system.
- Viruses will also try to infect the computer itself such as writing it self to the boot sector or running the entire system in a hyper-visor.
- Viruses often contain a payload which is to be activated at a future date to execute the intended action of the virus.
- Finding viruses can be done in two ways
  - Detect from time to time, scan the entire system.

  - Detect viruses when new files are added to the computer

- Signature based detection
  - A unique portion/characteristic of the program is used to form a signature of the virus which can be compared against a running list.
  - Viruses can be polymorphic and modify it self in order to ensure the signature does not match. As a result, signature doesn't really effect polymorphic protection
- Behaviour based detection
  - Behaviour based systems detect viruses by analysing its core-behaviour and purpose. They usually do this within a sandboxed environment.
- False Negative/Positives
  - Behaviour Detection has a tendency to have higher false positives.
  - Signature Detection has a tendency to have higher false negatives.
- False Positives must be lower than the base rate (The actual true percentage of viruses)

3.1.2.2 Worms

- A worm is a self-contained piece of code that can replicate with little or no user involvement
- Worms often use security flaws in widely deployed software as a path to infection
- Worms typically start searching for other computers to infect. Additionally, there may or may not be a payload that activates at a certain time or by another trigger.

3.1.2.3 Trojans

- Trojan horses are programs which claim to do something innocuous (and usually do), but which also hide malicious behaviour
- Often Gain control by getting the user to run code of the attackers choice, usually by also providing some code the user wants to run.
- Usually are marked as `PUP` (potentially unwanted programs)
- Trojan horses usually do not themselves spread between computers; they rely on multiple users executing the trojaned software