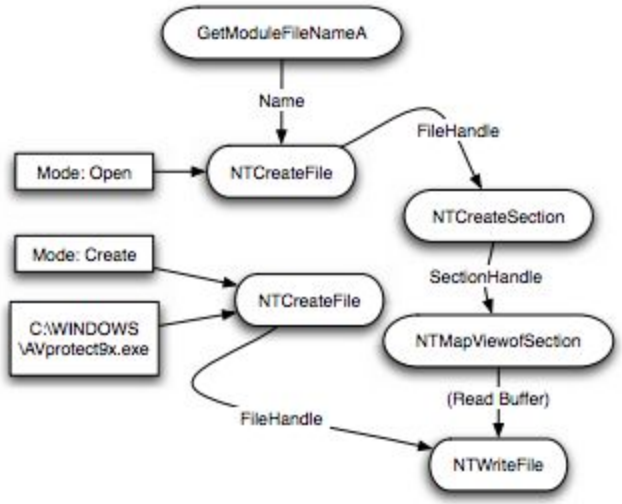
Tanish Arora
CS255 Computer Security

Q 1. What is random constant spread (RCS) model?
The RCS (Random Constant Spreading) worm has become one of the most malicious virus in recent computer networking circles. The worm has become a dominant, malicious virus in recent computer networking circles. The worm exhausts the resources of available CPU capacity, network peripherals and the transfer bandwidth causing damage to an uninfected system as well as an infected system. The worm selects an IP address randomly and infects it. The worm also progresses really rapidly in an exponential behavior.

2. Why Slammer spreads much faster than Code Red?
Slammer generates random IP addresses and patches itself to those IP, since they are really small in size its easy for them to get patched to their targets easily. With the advantage of being random/spontaneous in nature, it does not scan whether the target machine is running or not. Code-Red is latency limited, hence it needs a TCP connection and with the network latency the thread's scanning rate is limited thus making it less exponential growth than Slammer.

Q 3. Malware Detection paper: What are nodes and edges in the behavior graph?



As observed from the above graph, nodes represent system calls and edges represent the data dependency between any two system calls.

Q 4. How to they extract the data dependencies between system calls without dynamic data-flow (taint) analysis?
Data dependencies are analyzed by observing the data flow between two system calls and then knowing about the program only using the input -output data.

Q5. What are the requirements for transparent malware analysis?
In order to do the Transparent malware analysis, according to the paper there are a few things that need to be obtained such as the runtime behavior and the code should not include any side effects that are unconditionally detectable by the observation target. Other requirements that are mentioned in the paper are :

->Abstract Model of Program Execution
->Higher Privilege
->Identical Basic Instruction Execution Semantics
->Transparent Exception Handling

Q6. How does Ether intercept system calls outside the VM?
Ether is a malware analysis system which utilizes system hardware to intercept system calls which are made by malware and then extract that code. In order to intercept the system calls made by malware, ether replaces the value of malware system call to null, which forces the processor to trap the syscall. The information can later be derived from the CPU Logs.