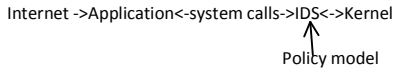


Intrusion Detection Systems

Monday, March 23, 2009
12:59 PM

- Host-based IDS vs Network IDS
- Monitor system calls to detect weird behavior



Policy - generic definition of allowed operations, applicable to untrusted code

- o Two metrics
 - False positives
 - False Negatives

Model - abstracted model of a specific apps behavior - applicable to trusted code

Generating Models

- Control flow graph (CFG) -> NDFA
 - o Static analysis approach
- Dynamic Analysis log
 - o Real traces as model
 - o Trace-based Intrusion Detection
 - Levenstein distance?
 - n-gram model
 - Example:
 - o T1: open, read, write, close
 - o T2: open, read, read, close
 - o T3: open, read, exec
 - o 3-gram
 - ◆ (open, read, write)
 - ◆ (read, write, close)
 - ◆ (open, read, exec)
 - ◆ (open, read, read)
 - ◆ (read, read, close)
 - Problems:
 - o False Positives
 - o Mimicry Attack could be used
 - ◆ Allowed traces should not overlap bad traces so a mimicry attack can take place
 - ◆ A trace between the bad and the allowed range would be the mimicry attack
 - Advantage:
 - o Can capture site-specific configuration

Efficient Context-Sensitive Intrusion Detection

- Track values flowing through program
- Tracked influence of syscall return vals on subsequent execution
- To improve performances app was rewritten to record it's path and report it to the IDS
- Worked on binaries

