Efficient Context-Sensitive Intrusion Detection Systems

Intrusion detection systems monitor the logs and draw the attention of authority to suspicious occurrences.

Our approach from the previous lecture turns out to be extremely impractical. This is because of how inefficient it is to make null calls for each function call we make.

Our next approach queues up all the state changes and hands them over to the IDS only on system calls.

```
null(2)  null(-3)
log(..)  null(5)
null(-2) log(..)
null(3)  null(-5)
log(..)
```

**Problem:** An attacker can manipulate the trace to his advantage!!
This type of attack is referred to as a mimicry attack!

**Mimicry Attack:** An attack where the bad guy makes his attack code imitate the correct behavior
Average time to accomplish a system takeover is between 12 and 300 syscalls!

Another nice thing about this is the average branching factor is ~1.05 where the branching factor is the number of children at each node.

From here we move on to our next topic of study,

**Sandboxes**
Goal: Give untrusted programs limited rights → principle of least privilege

IDS  
[APP] ↔ [Model]

vs.

Sandboxing  
[APP] ↔ [Policy] ← user