Host-Based Intrusion Detection System (IDS)

- Apps have some “normal” “behavior”
- Apps under attack will behave abnormally
- What is “normal”?
  - normal = expected
  - simplest model of behavior
  - normal behavior = set of possible syscall

While(1) {
  If(c==0)
    Getid();
  Else
    Write();
}  something error

-behavior
  => System calls made by app
Why sys calls?
1) Attacker must use sys calls to cause damage
2) Convenient point of mediation

M = model of normal behavior

If system finds attack, program will be killed instead of printing error message.

Evaluation Criteria
- Performance
- No/low FPs
- No/low Fns
- Manual
- Automatic from binaries
Model Construction

- Automatic from source -> 0 FP
- Automatic from execution traces
- A better model: order of syscalls
- n-gram mode

\[ M = \{ (, , , , ) , (, , , , ) \ldots \} \]

A sequence of system calls that application might perform

1. `Int main( ... )`

```c
{
  int fd = open();
  if (fd >= 0)
    read();
  else
    write();
  fork();
  close();
}
```

Chop the window

- (open,read)
- (open,write)
- (fork,close)
- (read,fork)
- (write,fork)

2. `Int main(...)`

```c
{
  int fd = open();
  if (fd >= 0)
    read();
  else
    write();
  fork();
  close();
  open();
  ioctl();
  close();
}
```

Chop the window

- (open,read)
- (open,write)
- (fork,open)
- (read,fork)
- (write,fork)
- (open,ioctl)
- (ioctl,close)