The list goes on

- Scanner can call setproctitle with user data
  Update daemon extracts data by running ps
- Scanner can bind particular TCP or UDP port numbers
  Sends no network traffic, but detectable by update daemon
- Scanner can relay data through another process (e.g ptrace) and exfiltrate data through yet another process (sendmail, httpd, portmap)
- Disclose data by modulating free disk space

Can we ever convince ourselves we have covered all possible communication channels (a.k.a covert channels)?

➡ Not without a more systematic approach to the problem

Mandatory Access Control Implementations

SELinux (Security Enhanced Linux)
enabled in major Linux distributions and Android

AppArmor
available in major Linux distributions

Smack (Simplified Mandatory Access Control Kernel)

Tomoyo Linux