Operating Systems Security III

CS 1660: Introduction to Computer Systems Security
=> How many of these can read your browser history?
.... all of them?!?!
.... all of them?!?!

deemer@ceres:~$ ls -la cookies.sqlite
rw-r-x--- 1 deemer deemer 9 Mar 12 16:40 cookies.sqlite

deemer@ceres$ some_random_app cookies.sqlite

... .

access("cookies.sqlite", F_OK) = 0
openat(AT_FDCWD, "cookies.sqlite", O_RDONLY) = 3
...

=> Access is just a syscall!
Works as long as permissions check out 😐
Owner of a resource decides on how it’s used

• Privileges depend on current user (and some groups)
• To elevate: admin user (root) vs. other users
Discretionary Access Control

Owner of a resource decides on how it’s used
• Privileges depend on current user (and some groups)
• To elevate: admin user (root) vs. other users

Is this really what we want?
How many of these *should* be able to read your browser history?  

*And why?*
Why?
Would like to get closer to...
Why?

• File permissions are very coarse
• Apps might not be trusted
• Apps might get compromised
Would like to get closer to...

Principle of Least Privilege
**Principle of Least Privilege**

An application should only be able to perform the operations necessary for its intended purpose
Isolation and Sandboxing

Run (untrusted) application in such a way that it has limited access to resources => only what it needs

Examples we’ve been discussing
Isolation and Sandboxing

Run (untrusted) application in such a way that it has limited access to resources => only what it needs

Examples we’ve been discussing

• Application sandboxing
• Namespaces (sort of)
• Containers (sort of)
• Virtual machines
Example: Gradescope
### Activity Monitor

#### My Processes

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Memory</th>
<th>Threads</th>
<th>Ports</th>
<th>PID</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finder</td>
<td>362.6 MB</td>
<td>6</td>
<td>1,402</td>
<td>720</td>
<td>deemer</td>
</tr>
<tr>
<td>Firefox</td>
<td>10.90 GB</td>
<td>162</td>
<td>1,404</td>
<td>785</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Service Worker</td>
<td>33.4 MB</td>
<td>32</td>
<td>109</td>
<td>12796</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>212.2 MB</td>
<td>29</td>
<td>121</td>
<td>1293</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>97.5 MB</td>
<td>29</td>
<td>106</td>
<td>1296</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>37.0 MB</td>
<td>28</td>
<td>110</td>
<td>1446</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>56.3 MB</td>
<td>28</td>
<td>111</td>
<td>1262</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>2.05 GB</td>
<td>33</td>
<td>139</td>
<td>1265</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>226.3 MB</td>
<td>30</td>
<td>124</td>
<td>1268</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>157.4 MB</td>
<td>28</td>
<td>119</td>
<td>1286</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>59.8 MB</td>
<td>28</td>
<td>103</td>
<td>1289</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>381.6 MB</td>
<td>29</td>
<td>119</td>
<td>1292</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>54.3 MB</td>
<td>28</td>
<td>103</td>
<td>1390</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>64.4 MB</td>
<td>28</td>
<td>102</td>
<td>1295</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>318.5 MB</td>
<td>28</td>
<td>112</td>
<td>1264</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>46.3 MB</td>
<td>28</td>
<td>111</td>
<td>1362</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>265.1 MB</td>
<td>30</td>
<td>130</td>
<td>1267</td>
<td>deemer</td>
</tr>
<tr>
<td>FirefoxCP Isolated Web Content</td>
<td>183.6 MB</td>
<td>34</td>
<td>137</td>
<td>1273</td>
<td>deemer</td>
</tr>
</tbody>
</table>

**Memory Pressure**
- Physical Memory: 32.00 GB
- Memory Used: 26.00 GB
- Cached Files: 5.96 GB
- App Memory: 13.22 GB
- Wired Memory: 2.54 GB
Example: web browsers

Browsers run a lot of untrusted code...

=> Worker processes that render pages run with fewer privileges
=> Site isolation: one process per site (or per tab)
Example: web browsers

Browsers run a lot of untrusted code...

=> Worker processes that render pages run with fewer privileges
=> Site isolation: one process per site (or per tab)

This protection is made possible by the following changes in Chrome's behavior:

- Cross-site documents are always put into a different process, whether the navigation is in the current tab, a new tab, or an iframe (i.e., one web page embedded inside another). Note that only a subset of sites are isolated on Android, to reduce overhead.
- Cross-site data (such as HTML, XML, JSON, and PDF files) is not delivered to a web page's process unless the server says it should be allowed (using CORS).
- Security checks in the browser process can detect and terminate a misbehaving renderer process (only on desktop platforms for the time being).

=> Can enforce Same-Origin Policy with separate processes!
How many of these should be able to read your browser history?
Typical desktop environment: User has a lot of freedom, can modify system

=> Built in an era where we weren’t downloading lots of untrusted code...
What if we could start over?
(sort of)
Mobile Operating System (iOS, Android)

=> Does user have root?
Mobile Operating Systems (iOS, Android)

=> Designed more as “secure by default” to restrict app privileges
Example: Android

• Based on Linux
• Many levels of application *sandboxing*
• Applications request permissions at installation and runtime
  => OS and Android Platform provides access

Nice writeups you can read:
- Android Security Paper 2023
- The Android Platform Security Model
Core sandboxing based on DAC

=> Every app gets its own user!

=> There is much more than this...
## Process list

<table>
<thead>
<tr>
<th>USER</th>
<th>PRI</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>S</th>
<th>%CPU</th>
<th>[%MEM</th>
<th>TIME+</th>
<th>ARGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>18</td>
<td>-2</td>
<td>22G</td>
<td>676M</td>
<td>523M</td>
<td>S</td>
<td>2.6</td>
<td>9.0</td>
<td>270:38.91</td>
<td>system_server</td>
</tr>
<tr>
<td>u0_a215</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>76M</td>
<td>51M</td>
<td>S</td>
<td>1.6</td>
<td>1.0</td>
<td>22:00.19</td>
<td>com.shannon.imsservice</td>
</tr>
<tr>
<td>shell</td>
<td>20</td>
<td>0</td>
<td>10G</td>
<td>5.5M</td>
<td>3.5M</td>
<td>R</td>
<td>1.3</td>
<td>0.0</td>
<td>0:01.10</td>
<td>top</td>
</tr>
<tr>
<td>u0_a167</td>
<td>20</td>
<td>0</td>
<td>34G</td>
<td>328M</td>
<td>215M</td>
<td>S</td>
<td>1.0</td>
<td>4.4</td>
<td>0:39.46</td>
<td>com.google.android.googlequa</td>
</tr>
<tr>
<td>u0_a215</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>59M</td>
<td>39M</td>
<td>S</td>
<td>1.0</td>
<td>0.7</td>
<td>1:28.44</td>
<td>ShannonImsService</td>
</tr>
<tr>
<td>system</td>
<td>20</td>
<td>0</td>
<td>10G</td>
<td>2.7M</td>
<td>2.4M</td>
<td>S</td>
<td>1.0</td>
<td>0.0</td>
<td>38:17.24</td>
<td>android.hardware.power.stats</td>
</tr>
<tr>
<td>u0_a87</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>68M</td>
<td>48M</td>
<td>S</td>
<td>0.6</td>
<td>0.9</td>
<td>0:00.10</td>
<td>com.android.providers.calendar</td>
</tr>
<tr>
<td>radio</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>117M</td>
<td>66M</td>
<td>S</td>
<td>0.6</td>
<td>1.5</td>
<td>18:55.63</td>
<td>com.android.phone</td>
</tr>
<tr>
<td>u0_a233</td>
<td>0</td>
<td>0</td>
<td>18G</td>
<td>297M</td>
<td>165M</td>
<td>S</td>
<td>0.6</td>
<td>3.9</td>
<td>56:24.60</td>
<td>com.android.systemui</td>
</tr>
</tbody>
</table>
| root          | 20  | 0  | 0     | 0    | 0   | I  | 0.3  | 0.0   | 0:00.56 | [kworker/u16:5-cp2ap_wakeup_wq]
| root          | 20  | 0  | 0     | 0    | 0   | I  | 0.3  | 0.0   | 0:00.51 | [kworker/u16:3-events_unbound]
| u0_a343       | 20  | 0  | 17G   | 102M | 70M | S  | 0.3  | 1.3   | 4:20.28  | com.whatsapp                |
| u0_a207       | 20  | 0  | 22G   | 52M  | 37M | S  | 0.3  | 0.6   | 13:55.88 | com.google.android.connectiv|
| radio         | 20  | 0  | 11G   | 5.8M | 5.8M| S  | 0.3  | 0.0   | 5:09.88  | rild_exynos                 |
| root          | RT  | 0  | 0     | 0    | 0   | S  | 0.3  | 0.0   | 3:51.72  | [sugov:6]                   |
| root          | RT  | 0  | 0     | 0    | 0   | S  | 0.3  | 0.0   | 27:11.68 | [sugov:0]                   |
| system        | 20  | 0  | 10G   | 2.8M | 2.1M| S  | 0.3  | 0.0   | 8:07.16  | servicemanager              |

Tasks: 907 total, 1 running, 906 sleeping, 0 stopped, 0 zombie
Mem: 7618164K total, 7339296K used, 278868K free, 3240K buffers
Swap: 3145724K total, 2944924K used, 200800K free, 2456224K cached
%cpu 5%user 1%nice 8%sys 785%idle 0%iow 1%irq 1%sirq 0%host
### Process List

**Tasks:** 907 total, 1 running, 906 sleeping, 0 stopped, 0 zombie

**Mem:** 7618164K total, 7339296K used, 278868K free, 3240K buffers

**Swap:** 3145724K total, 2944924K used, 200800K free, 2456224K cached

<table>
<thead>
<tr>
<th>USER</th>
<th>PR</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>S</th>
<th>%CPU</th>
<th>[%MEM]</th>
<th>TIME+</th>
<th>ARGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>76M</td>
<td>51M</td>
<td>S</td>
<td>1.6</td>
<td>1.0</td>
<td>22:00.19</td>
<td>top</td>
</tr>
<tr>
<td>shell</td>
<td>20</td>
<td>0</td>
<td>10G</td>
<td>5.5M</td>
<td>3.5M</td>
<td>R</td>
<td>1.3</td>
<td>0.0</td>
<td>0:01.10</td>
<td>com.shannon.imsservice</td>
</tr>
<tr>
<td>u0_a167</td>
<td>20</td>
<td>0</td>
<td>34G</td>
<td>328M</td>
<td>215M</td>
<td>S</td>
<td>1.0</td>
<td>4.4</td>
<td>0:39.46</td>
<td>com.google.android.googlequicksearchbox:search</td>
</tr>
<tr>
<td>u0_a215</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>59M</td>
<td>39M</td>
<td>S</td>
<td>1.0</td>
<td>0.7</td>
<td>1:28.44</td>
<td>ShannonImsService</td>
</tr>
<tr>
<td>system</td>
<td>20</td>
<td>0</td>
<td>10G</td>
<td>2.7M</td>
<td>2.4M</td>
<td>S</td>
<td>1.0</td>
<td>0.0</td>
<td>38:17.24</td>
<td>android.hardware.power.stats</td>
</tr>
<tr>
<td>u0_a87</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>63M</td>
<td>48M</td>
<td>S</td>
<td>0.6</td>
<td>0.9</td>
<td>0:00.10</td>
<td>com.android.providers.calendar</td>
</tr>
<tr>
<td>radio</td>
<td>20</td>
<td>0</td>
<td>16G</td>
<td>117M</td>
<td>66M</td>
<td>S</td>
<td>0.6</td>
<td>1.5</td>
<td>18:55.63</td>
<td>com.android.phone</td>
</tr>
<tr>
<td>u0_a233</td>
<td>20</td>
<td>0</td>
<td>18G</td>
<td>297M</td>
<td>165M</td>
<td>S</td>
<td>0.6</td>
<td>3.9</td>
<td>56:24.60</td>
<td>com.android.systemui</td>
</tr>
<tr>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>I</td>
<td>0.3</td>
<td>0.0</td>
<td>0:00.56</td>
<td>[kworker/u16:5-cp2ap_wakeup]</td>
</tr>
<tr>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>I</td>
<td>0.3</td>
<td>0.0</td>
<td>0:00.51</td>
<td>[kworker/u16:3-events_unbound]</td>
</tr>
<tr>
<td>u0_a343</td>
<td>20</td>
<td>0</td>
<td>17G</td>
<td>102M</td>
<td>70M</td>
<td>S</td>
<td>0.3</td>
<td>1.3</td>
<td>4:20.28</td>
<td>com.whatsapp</td>
</tr>
<tr>
<td>u0_a207</td>
<td>20</td>
<td>0</td>
<td>22G</td>
<td>52M</td>
<td>37M</td>
<td>S</td>
<td>0.3</td>
<td>0.6</td>
<td>13:55.88</td>
<td>com.google.android.connectivitythermalpowermanager</td>
</tr>
<tr>
<td>radio</td>
<td>20</td>
<td>0</td>
<td>11G</td>
<td>5.8M</td>
<td>5.8M</td>
<td>S</td>
<td>0.3</td>
<td>0.0</td>
<td>5:09.88</td>
<td>rild_exynos</td>
</tr>
<tr>
<td>root</td>
<td>RT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.3</td>
<td>0.0</td>
<td>3:51.72</td>
<td>[sugov:6]</td>
</tr>
<tr>
<td>root</td>
<td>RT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0.3</td>
<td>0.0</td>
<td>27:11.68</td>
<td>[sugov:0]</td>
</tr>
<tr>
<td>system</td>
<td>20</td>
<td>0</td>
<td>10G</td>
<td>2.8M</td>
<td>2.1M</td>
<td>S</td>
<td>0.3</td>
<td>0.0</td>
<td>8:07.16</td>
<td>servicemanager</td>
</tr>
</tbody>
</table>
Allow VLC to access photos, media, and files on your device?

Allow
Deny

Allow “Maps” to access your location while you are using the app?

Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.

Allow While Using App
Allow Once
Don’t Allow
Examining an app...

requested permissions:
  - android.permission.ACCESS_WIFI_STATE
  - android.permissionINTERNET
  - android.permission.ACCESS_NETWORK_STATE
  - android.permission.WAKE_LOCK
  - android.permission.GET_ACCOUNTS
  - android.permission.RECEIVE_BOOT_COMPLETED

install permissions:
  com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE: granted=true
  com.google.android.c2dm.permission.RECEIVE: granted=true
  android.permission.USE_CREDENTIALS: granted=true
  android.permission.MODIFY_AUDIO_SETTINGS: granted=true
  android.permission.FOREGROUND_SERVICE: granted=true
  android.permission.CHANGE_WIFI_STATE: granted=true
  android.permission.FOREGROUND_SERVICE_DATA_SYNC: granted=true
  android.permission.ACCESS_NETWORK_STATE: granted=true
  android.permission.USE_FINGERPRINT: granted=true
  android.permission.READ_BASICPHONE_STATE: granted=true
**SELinux Policies on resources**

```
$ ls -laZ

lrw-r--r-- 1 root root   u:object_r:rootfs:s0       11 bin -> /system/bin
drwxr-xr-x 2 root root   u:object_r:tmpfs:s0       4096 debug_ramdisk
drwxr-xr-x 24 root root   u:object_r:device:s0      160 dev
drwxr-xr-x 13 root shell  u:object_r:vendor_file:s0  4096 vendor
drwxr-xr-x  5 root root   u:object_r:vendor_file:s0  4096 vendor_dlkm
drwx---x--- 4 shell everybody u:object_r:mnt_user_file:s0  80 storage
```

```bash
$ sesearch -A selinux_policy

allow adbd adb_keys_file:dir search;
allow adbd adb_keys_file:file { getattr ioctl lock map open read watch watch_reads };
```
access("cookies.sqlite", F_OK) = 0  
openat(AT_FDCWD, "cookies.sqlite", O_RDONLY) = 3

=> Fine-grained permissions at runtime!

Allow "Maps" to access your location while you are using the app?
Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.

Allow While Using App
- Allow Once
- DON'T Allow
...at compile time?
Other ways?

• What does it mean for the user to be "unprivileged"?

• What does it mean for code run by a user to be "unprivileged"?

• What do we want that code to be able to do?

  => How much do we trust the user? The code?
Other ways?

• What does it mean for the user to be "unprivileged"?

• What does it mean for code run by a user to be "unprivileged"?

• What do we want that code to be able to do?

  => How much do we trust the user? The code?

• sudo is pretty coarse-grained...