Grafting Apple Tree’s
Building a useful process tree
Jaron Bradley
Detection R&D
Jamf Protect
Incident Response and the Process Tree
Standard Tree

- **launchd**
  - **PID**: 1

  - **Google Chrome.app**
    - **PID**: 123
    - **PPID**: 1
  - **Calculator.app**
    - **PID**: 125
    - **PPID**: 1
  - **Calendar.app**
    - **PID**: 130
    - **PPID**: 1
  - **Terminal.app**
    - **PID**: 134
    - **PPID**: 1

- **Google Chrome Helper**
  - **PID**: 124
  - **PPID**: 123
A More Useful Tree

- **launchd**
  - **PID: 1**
  - **Spotlight.app**
    - **PID: 177**
    - **PPID: 1**
  - **Dock.app**
    - **PID: 235**
    - **PPID: 1**
  - **Finder.app**
    - **PID: 29**
    - **PPID: 1**
  - **Calculator.app**
    - **PID: 1237**
    - **PPID: 125**
  - **Calendar.app**
    - **PID: 1303**
    - **PPID: 130**
  - **Google Chrome.app**
    - **PID: 1234**
    - **PPID: 123**
  - **Terminal.app**
    - **PID: 1304**
    - **PPID: 1**
Launchctl Procinfo

bsd proc info = {
    pid = 34442
    unique pid = 34442
    pgid = 34442
    status = stopped
    flags = 64-bit has controlling tty has controlling terminal
    uid = 501
    svuid = 501
    ruid = 501
    gid = 20
    svgid = 20
    rgid = 20
    comm name = zsh
    long name = zsh
    controlling tty devnode = 0x10000005
    controlling tty pgid = 34442
}

audit info
    session id = 100221
    uid = 501
    success mask = 0x30000
    failure mask = 0x30000
    flags = has_graphic_access, has tty, has console access, has authenticated

sandboxed = no
container = (no container)

responsible pid = 34316
responsible unique pid = 34316
responsible path = /Applications/iTerm.app/Contents/MacOS/iTerm2

pressured exit info = {
    dirty state tracked = 0
    dirty = 0
    pressured-exit capable = 0
}
### Responsible Pid

<table>
<thead>
<tr>
<th>Process Name</th>
<th>Pid</th>
<th>CPU</th>
<th>Memory</th>
<th>Threads</th>
<th>Status</th>
<th>Priority</th>
<th>User</th>
<th>Group</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slack</td>
<td>1377</td>
<td>0.1</td>
<td>4:27.42</td>
<td>32</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack Helper (Renderer)</td>
<td>1438</td>
<td>0.6</td>
<td>2:12.55</td>
<td>21</td>
<td>5</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack Helper (GPU)</td>
<td>1412</td>
<td>0.4</td>
<td>6:13.37</td>
<td>10</td>
<td>5</td>
<td>0.1</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack Helper</td>
<td>2658</td>
<td>0.0</td>
<td>39.74</td>
<td>10</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slack Helper</td>
<td>1432</td>
<td>0.0</td>
<td>62.57</td>
<td>7</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.apple.audio.SandboxHelper</td>
<td>2659</td>
<td>0.0</td>
<td>0.01</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.apple.audio.SandboxHelper</td>
<td>1464</td>
<td>0.0</td>
<td>0.08</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTDestructorXPCService</td>
<td>1439</td>
<td>0.0</td>
<td>0.06</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SystemUIServer</td>
<td>1393</td>
<td>0.1</td>
<td>8.04</td>
<td>4</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTLCompilerService</td>
<td>3594</td>
<td>0.0</td>
<td>0.05</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>screen capture</td>
<td>6131</td>
<td>0.12</td>
<td>0.12</td>
<td>3</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fsevents.d</td>
<td>116</td>
<td>0.1</td>
<td>1:15.51</td>
<td>2</td>
<td>0</td>
<td>0.0</td>
<td>root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UserEventAgent</td>
<td>515</td>
<td>0.1</td>
<td>6.98</td>
<td>3</td>
<td>0</td>
<td>0.0</td>
<td>jbradley</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To find the responsible Pid:

```
jbradley@phistafunk Debug % ps -eo pid,ppid,command= | grep 2939 | grep -v grep 2939 | /System/Library/Frameworks/AudioToolbox.framework/XPCServices/com.apple.audio.SandboxHelper.xpc/Contents/MacOS/com.apple.audio.SandboxHelper
```

Result:

```
```
$ sudo launchctl procinfo 2939

bsd proc info = {
    pid = 2939
    unique pid = 2939
    ppid = 1  Wat?
    pgid = 2939
}
responsible pid = 1377  heh?
responsible unique pid = 1377
responsible path = /Applications/Slack.app/Contents/MacOS/Slack

Responsible Pid
Responsible Pid

No PPID option!?
com.apple.xpc.launchd.oneshot.0x10000008.Messages = {
  active count = 4
  copy count = 0
  one_shot = 1
  path = (submitted by loginwindow.187)
  state = running
  bundle id = com.apple.icChat

  program = /System/Applications/Messages.app/Contents/MacOS/Messages
  arguments = {
    /System/Applications/Messages.app/Contents/MacOS/Messages
    -psn_0_110619
  }

  inherited environment = {
    SSH_AUTH_SOCK => /private/tmp/com.apple.launchd.D8IFhICj0oY/Listeners
  }

  default environment = {
    PATH => /usr/bin:/bin:/usr/sbin:/sbin
  }
}
com.apple.Dock.agent = {
    active count = 14
    copy count = 0
    one shot = 0
    path = /System/Library/LaunchAgents/com.apple.Dock.plist
    state = running
}
Dead Pids as Parents

```python
com.googlecode.iterm2.17084 = {
    active count = 5
    copy count = 0
    one shot = 0
    path = (submitted by Autoupdate.37758)
    state = running
    bundle id = com.googlecode.iterm2

    program = /Applications/iTerm.app/Contents/MacOS/iTerm2
    arguments = {
        /Applications/iTerm.app/Contents/MacOS/iTerm2
    }
}
```

```bash
$ sudo launchctl procinfo 37758
program path = (could not resolve path)
Could not print Mach info for pid 37758: 0x5
Could not get proc info PID 37758: 3: No such process
auditon: 3: No such process
Could not get responsible PID for PID 37758: 3: No such process
proc_get_dirty(): 3: No such process
entitlements = (no entitlements)
Could not get code signing info: 3: No such process
(pid 37758 is not managed by launchd)
```

```bash
$ ```
Filling in the Blanks - Fork/Exec

Launchd
Pid: 1

ProcessA
Pid: 2

ProcessB
Pid: 3
Filling in the Blanks -> Fork

Launchd
Pid: 1

ProcessA
Pid: 2

ProcessA
Pid: 3

Fork
Filling in the Blanks -> Exec

Launchd
Pid: 1

ProcessB
Pid: 3
Filling in the Blanks -> Fork+Exec

1. Launchd (Pid: 1)
2. ProcessA (Pid: 2)
3. Fork/Exec
4. ProcessB (Pid: 3)
Finding True Parents of Exec’ed Parents

- Launchd
  - Pid: 1

- ProcessB
  - Pid: 2

- ProcInfo

- Exec
Introducing TrueTree

- Command Line Based
- Lightweight
- Fast
- Open Source Swift
- “Post Mortem” Analysis
- Great for IR Engagements
- Requires Root :(
TrueTree --standard

/sbin/launchd  1
/System/Library/Frameworks/QuickLook.framework/Versions/A/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite  585
/Applications/VMware Fusion.app/Contents/Library/vmnet-netifup  15883
/usr/libexec/ld  258
/usr/libexec/nsurlsessiond  260
/usr/libexec/seld  16336
/System/Library/PrivateFrameworks/PackageKit.framework/Versions/A/Resources/systeminstalld  997
/System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService  1567
/usr/libexec/trustd  270
/System/Library/PrivateFrameworks/UserActivity.framework/Agents/useractivityd  474
TrueTree

/System/Library/LaunchDaemons/ssh.plist
/usr/libexec/sshd-keygen-wrapper (Exec'ed into below process) 50010
/usr/sbin/sshd 50010
/usr/sbin/sshd 50014
/bin/zsh 50015
/bin/dash 50018
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/Resources/com.apple.SafariCloudHistoryPushAgent.plist
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/MacOS/SafariCloudHistoryPushAgent 12015
/Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign 10672
/System/Library/Input Methods/PressAndHold.app/Contents/PlugIns/PAH_Extension.appex/Contents/MacOS/PAH_Extension 515
/System/Library/LaunchDaemons/com.apple.oscpd.plist
/usr/sbin/oscpd 11870
/System/Library/PrivateFrameworks/GeoServices.framework/Versions/A/XPCServices/com.apple.qeod.xpc/Contents/MacOS/com.apple.qeod 261
/Applications/Cisco Webex Meetings.app/Contents/MacOS/Cisco Webex Meetings (TrueParent:46639 "PTUpdate" has Terminated)
/Applications/Cisco Webex Meetings.app/Contents/PlugIns/webextma.app/Contents/MacOS/webextma 46712
/Applications/Cisco Webex Meetings.app/Contents/MacOS/CiscoSparkHelper 46743
/System/Library/LaunchAgents/com.apple.parsecd.plist
/System/Library/PrivateFrameworks/CoreParsec.framework/parsecd 441
<table>
<thead>
<tr>
<th>Directory</th>
<th>Timestamps</th>
</tr>
</thead>
<tbody>
<tr>
<td>/sbin/launchd</td>
<td>2020-02-11 02:09:27 +0000</td>
</tr>
<tr>
<td>/System/Library/LaunchDaemons/com.apple.MobileFileIntegrity.plist</td>
<td>2020-02-11 02:09:36 +0000</td>
</tr>
<tr>
<td>/usr/libexec/amfd</td>
<td>2020-02-11 02:09:36 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreMediaIO.framework/Versions/A/XPCServices/com.apple.cmio.registerassistantservice.xpc/Contents/MacOS/com.apple.cmio.registerassistantservice</td>
<td>2020-02-11 02:09:36 +0000</td>
</tr>
<tr>
<td>/System/Library/LaunchDaemons/com.apple.opendirectory.plist</td>
<td>2020-02-11 02:09:36 +0000</td>
</tr>
<tr>
<td>/usr/libexec/opendirectory</td>
<td>2020-02-11 02:09:36 +0000</td>
</tr>
<tr>
<td>/System/Library/LaunchAgents/com.apple.cache_delete.plist</td>
<td>497 2020-02-11 02:09:52 +0000</td>
</tr>
<tr>
<td>/System/Library/PrivateFrameworks/CacheDelete.framework/deleted</td>
<td>497 2020-02-11 02:09:52 +0000</td>
</tr>
<tr>
<td>/System/Library/LaunchAgents/com.apple.mdworker.shared.plist</td>
<td>2244 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2244 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>1290 2020-02-11 02:12:54 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2246 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>1994 2020-02-11 03:31:24 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2338 2020-02-11 04:13:37 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2033 2020-02-11 03:35:52 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2124 2020-02-11 03:41:36 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2242 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2242 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>1816 2020-02-11 03:14:36 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2133 2020-02-11 03:47:55 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2339 2020-02-11 04:13:37 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2243 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>2245 2020-02-11 04:09:58 +0000</td>
</tr>
<tr>
<td>/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared</td>
<td>1991 2020-02-11 03:38:58 +0000</td>
</tr>
</tbody>
</table>
Use Case - Dock
Use Case - Spotlight
Use Case - Finder TrueTree
Use Case - Login Windows

/System/Library/LaunchDaemons/com.apple.loginwindow.plist 185
/Applications/Spotify.app/Contents/MacOS/Spotify 519
/System/Library/CoreServices/loginwindow.app/Contents/MacOS/loginwindow 500
/System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService 13131
/System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService 1544
/System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService 1567
/System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService 1545
/System/Library/Frameworks/VideoToolbox.framework/Versions/A/XPCServices/VTDecoderXPCService.xpc/Contents/MacOS/VTDecoderXPCService 576
/System/Library/Frameworks/AppKit.framework/Versions/C/XPCServices/SandboxedServiceRunner.xpc/Contents/MacOS/SandboxedServiceRunner 1334
/Applications/Slack.app/Contents/Frameworks/Slack Helper (Renderer).app/Contents/MacOS/Slack Helper (Renderer) 15232
/Applications/Slack.app/Contents/Frameworks/Slack Helper (GPU).app/Contents/MacOS/Slack Helper (GPU) 564
Use Case - Open

/Applications/Safari.app/Contents/MacOS/Safari (TrueParent:16095 "open" has Terminated)
Use Case - AppleScript
Use Case - SSH Standard
Use Case - SSH TrueTree

/System/Library/LaunchDaemons/ssh.plist
  /usr/libexec/sshd-keygen-wraper (Exec'ed into below process) 50010
  /usr/sbin/sshd 50010
  /usr/sbin/sshd 50014
  /bin/zsh 50015
  /bin/dash 50018

/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/Resources/com.apple.SafariCloudHistoryPushAgent.plist
  Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/MacOS/SafariCloudHistoryPushAgent 12015

/Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign 10672

/System/Library/Input Methods/PressAndHold.app/Contents/PlugIns/PAH_Extension.appex/Contents/MacOS/PAH_Extension 515

/System/Library/LaunchDaemons/com.apple.oscpd.plist
  /usr/sbin/oscpd 11870

/System/Library/PrivateFrameworks/GeoServices.framework/Versions/A/XPCServices/com.apple.geod.xpc/Contents/MacOS/com.apple.geod 261

/Applications/Cisco Webex Meetings.app/Contents/MacOS/Cisco Webex Meetings (TrueParent:46639 "PTUpdate" has Terminated)

/Applications/Cisco Webex Meetings.app/Contents/PlugIns/webexmta.app/Contents/MacOS/webexmta 46712

/Applications/Cisco Webex Meetings.app/Contents/MacOS/CiscoSparkHelper 46743

/System/Library/LaunchAgents/com.apple.parsecd.plist
  /System/Library/PrivateFrameworks/CoreParsec.framework/parsecd 441
Use Case - SSH Enabled
Use Case - Launchctl Standard

launchctl submit -l com.evil.whatever -- calculator.app
Use Case - Launchctl TrueTree

/sbin/launchd  1
/System/Library/LaunchDaemons/com.apple.sysmond.plist
 /usr/libexec/sysmond  362
/System/Library/LaunchAgents/com.apple.trustd.agent.plist
 /usr/libexec/trustd  270
 /usr/libexec/trustd  410
 /usr/libexec/trustd  1003
/System/Applications/Calculator.app/Contents/MacOS/Calculator (TrueParent:16527 "launchctl" has Terminated)
/System/Library/LaunchAgents/com.apple.AMPLibraryAgent.plist
 /System/Library/PrivateFrameworks/AMPLibrary.framework/Versions/A/Support/AMPLibraryAgent  520
/System/Library/LaunchDaemons/com.apple.kextd.plist
 /usr/libexec/kextd  113
/System/Library/PrivateExtensions/AppleHIDDrivers.dskk/AppleHIDDrivers  45555
Use Case - Office Macros Standard
Use Case - Time Based Assumptions
Use Case - WindTail

Do you want to allow this page to open “Terminal”?

Cancel  Allow

NAME
whoami (1) - BSD General Commands Manual

SYNOPSIS
whoami

DESCRIPTION
The whoami utility has been obsoleted by the id(1) utility, and is equivalent to “id -un”. The command “id -p” is suggested for normal interactive use.

The whoami utility displays your effective user ID as a name.

EXIT STATUS
The whoami utility exits 0 on success, and >0 if an error occurs.

SEE ALSO
id(1)

BSD       June 6, 1993

[Process completed]
Use Case - URLScheme (Safari) Standard
Use Case - URLScheme (Safari)
Use Case - URLScheme (Chrome)
ms-excel:ofv|u|http://127.0.0.1:8000/hax.xlsm

1.5 COMMAN

View Document

The following command will cause the application to open the document referenced by the command.

Command Name: ofv

Command argument descriptor: u

Command argument: a URI to the document, based on the http or https scheme

Example: ms-excel:ofv|u|https://contoso/Q4/budget.xls
Use Case - URLScheme + Office Macro (Chrome) Standard
TrueTree is available for download

www.themittenmac.com

Source Code available on GitHub

Special Thanks:
Jonathan Levin
Patrick Wardle
Cyrus Ingraham
Josh Stein
Thank you