Capsicum working group summary

Robert N.M. Watson
University of Cambridge

FreeBSD Developer Summit
7 October 2011 - Maarssen, The Netherlands
Capsicum

- Lightweight operating system capability and sandbox framework
- Kernel features appear in FreeBSD 9.0
- Application compartmentalisation
- Supplements existing DAC/MAC
- Collaboration between Cambridge, Google
Working group goals

- Capability ioctl whitelists
- Sandboxed DNS and other services
- Migrating to privilege upgrade from privilege downgrade
- Updating Chromium patches
- libcapsicum
- 9.1 agenda
- connectat(), bindat()
- pdwait()
- Brainstorm applications to compartmentalise
ioctl white-listing

- Motivation: pjdü’s work on hastd
- ioctl is message passing
  - Thousands of calls with diverse semantics
  - Can’t interpret at system call boundary
- Currently we have CAP_IOCTL
  - Idea: add white list table
  - Only white-listed ioctls available without CAP_IOCTL
- Discussion: masks, groups, …
- Conclusion: keep it simple for now
Missing system calls

- bindat(), connectact()
- [f]chflagsat()
- pdtrace()
- What about pdwait4()?
- Can we lose reparenting?
Other system features

- Socket option white-listing
- fcntl white-listing
- cwd as a capability
- close-on-exec for process descriptors
- Kill on ECAPMODE
- Core dumping to descriptor/socket
Services to offer to sandboxes

- Capsicum Services Daemon (CSD) -- launchd?
- Services for (and in) sandboxes
  - sysctl -- think compartmentalised netstat/sockstat/top/...
  - DNS, DNSSEC
  - Sockets, files … ftsat(3)?
  - SSL client/server
  - Authentication services
  - Various nscd services (or not)
- Requires us to clean up Capsicum’s fdlist but good starting point
FreeBSD things to sandbox

<table>
<thead>
<tr>
<th>Package</th>
<th>Package</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpcbind, mountd</td>
<td>wpa_supplicant</td>
<td>finger, fingerd</td>
</tr>
<tr>
<td>SSH client, server</td>
<td>all setuid binaries</td>
<td>openssl</td>
</tr>
<tr>
<td>libfetch</td>
<td>snmpd</td>
<td>grep, awk, head, tail, …</td>
</tr>
<tr>
<td>libarchive (bsdtar)</td>
<td>trsold, routed, …</td>
<td>bc</td>
</tr>
<tr>
<td>zlib (gzip)</td>
<td>named</td>
<td>man</td>
</tr>
<tr>
<td>ftpd, tftpd</td>
<td>ntpd</td>
<td>od/hexdump</td>
</tr>
<tr>
<td>bootpd</td>
<td>lwresd</td>
<td>csup</td>
</tr>
<tr>
<td>inetd</td>
<td>Kerberos, kadmind</td>
<td>pkgng</td>
</tr>
<tr>
<td>netcat</td>
<td>rwhod</td>
<td></td>
</tr>
<tr>
<td>syslogd</td>
<td>file, libmagic</td>
<td></td>
</tr>
</tbody>
</table>
Ports we want sandboxed*

- KDE - IO slaves
- PDF viewer! (xdpdf?)
- BIND
- Apache
- Sendmail
- Chromium (update)
- nginx
- Unbound
- Varnish
- Mozilla

- lighttpd
- ImageMagick
- Subversion
- git
- Dovecot
- OpenLDAP
- Cyrus
- Spamassassin
- ClamAV
- mplayer

* notice aggressive use of passive voice
The plan

- 9.0: features present but not in GENERIC
- 9.1: Enable in GENERIC!
  - libcapsicum(3), csd(8)
  - Selected security-critical applications
    - SSH, dhclient, tcpdump, BIND, inetd, ...