IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Assessing the Linux Desktop's Security

Ilja van Sprundel <ivansprundel@ioactive.com>
Shane Macaulay <shane.macaulay@ioactive.com>

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Who am I?

- IOActive
- Director of Penetration Testing
- Pentest
- Code review
- Break stuff for fun and profit ☺

agenda

- Intro
- Observations
- Problems
- More observations
- More problems summary
- Solutions ?

What this talk is about

- Local security of linux on the desktop

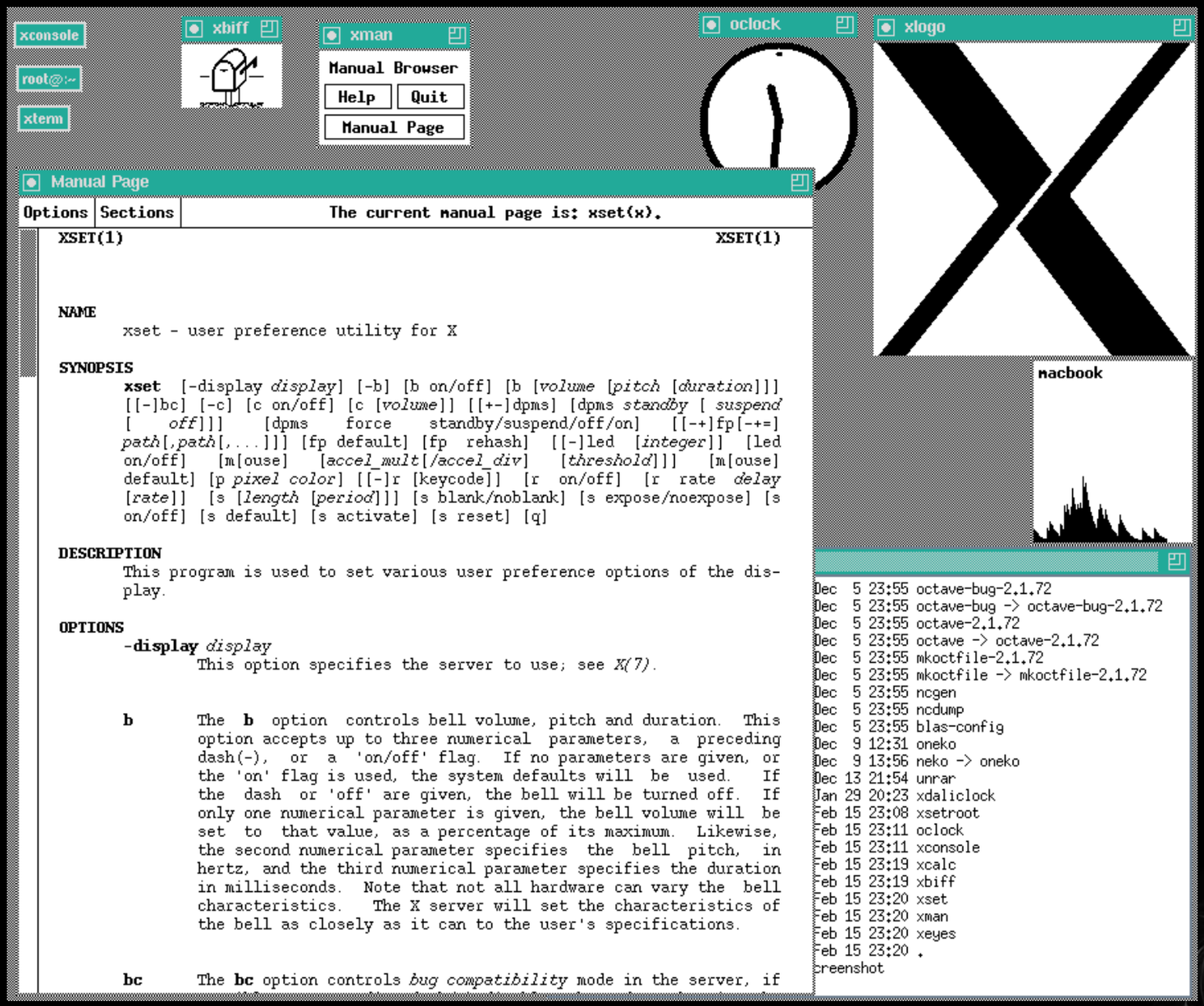
Intro

- Used to use linux as my main desktop machine
- Switched to windows about 7 years ago
  - Mainly for work reasons
- Have used linux sporadically since then
  - However, not as a desktop OS
- Things seem to have changed somewhat

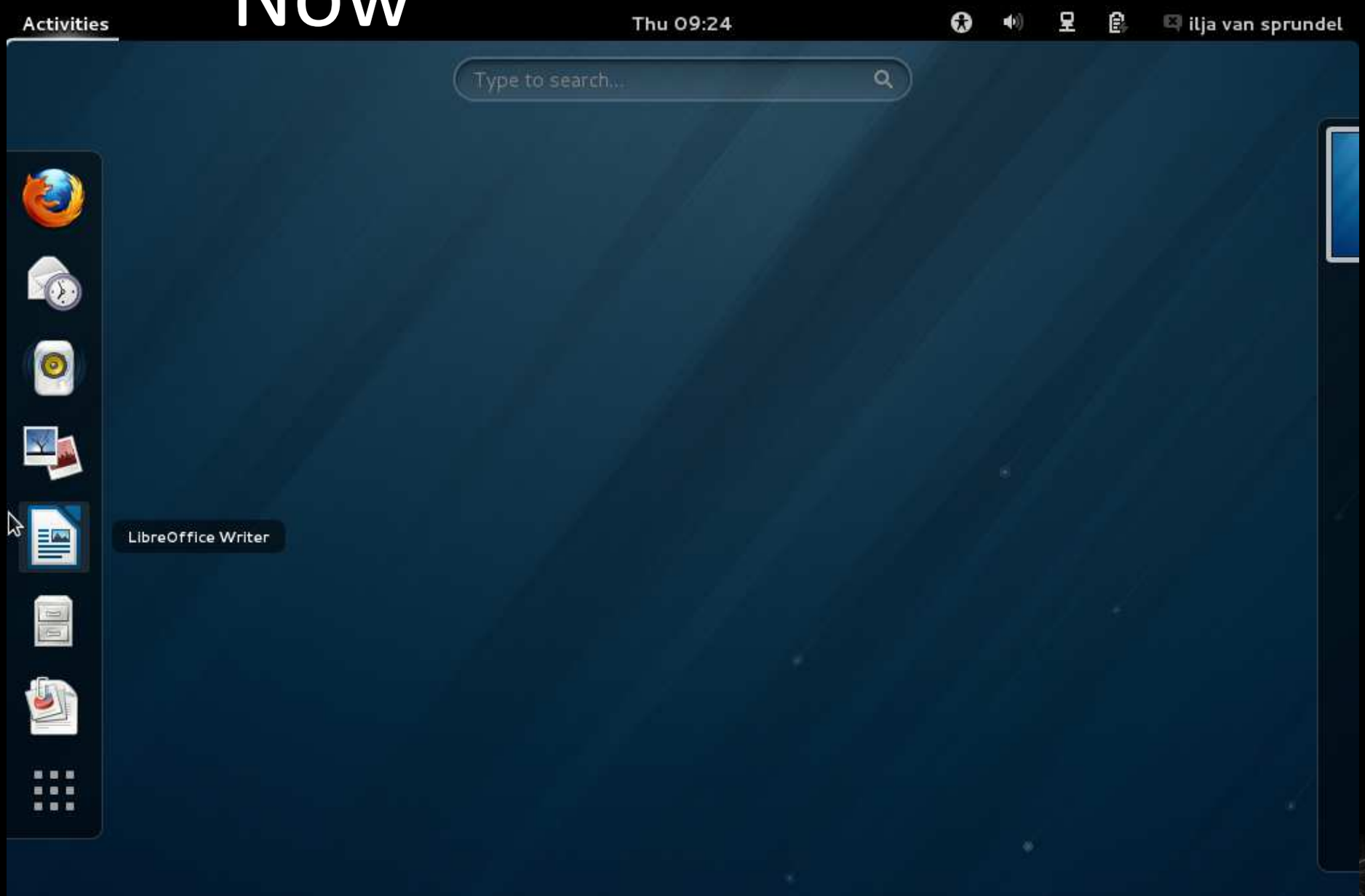
Intro

- Installed ubuntu during the holidays last year
- Boots into a gui, looks like some mix of windows and osx gui
- It's pretty clear they want to matter as a desktop os
  - 7-10 years ago, it looked like, well, X
  - Today, it looks like something my grandmother can use
- Also looked at fedora, opensuse, knoppix
- Also took a quick look at osx and opensolaris (openindiana)

A decade ago


xconsole
root@:~
xterm
xbiff
xman
Manual Browser
Help
Quit
Manual Page
oclock
xlogo
Manual Page
Options
Sections
The current manual page is: xset(x).
XSET(1)
XSET(1)
NAME
xset - user preference utility for X
SYNOPSIS
xset [-display display] [-b] [b on/off] [b [volume [pitch [duration]]] [[-]bc] [-c] [c on/off] [c [volume]] [[+-]dpms] [dpms standby [suspend [off]]] [dpms force standby/suspend/off/on] [[-+]fp[-+=] path[,path[,...]]] [fp default] [fp rehash] [[-]led [integer]] [led on/off] [m[ouse] [accel_mult[/accel_div] [threshold]]] [m[ouse] default] [p pixel color] [[-]r [keycode]] [r on/off] [r rate delay [rate]] [s [length [period]]] [s blank/noblank] [s expose/noexpose] [s on/off] [s default] [s activate] [s reset] [q]
DESCRIPTION
This program is used to set various user preference options of the display.
OPTIONS
-display display
This option specifies the server to use; see X(7).
b
The b option controls bell volume, pitch and duration. This option accepts up to three numerical parameters, a preceding dash(-), or a 'on/off' flag. If no parameters are given, or the 'on' flag is used, the system defaults will be used. If the dash or 'off' are given, the bell will be turned off. If only one numerical parameter is given, the bell volume will be set to that value, as a percentage of its maximum. Likewise, the second numerical parameter specifies the bell pitch, in hertz, and the third numerical parameter specifies the duration in milliseconds. Note that not all hardware can vary the bell characteristics. The X server will set the characteristics of the bell as closely as it can to the user's specifications.
bc
The bc option controls bug compatibility mode in the server, if
macbook
Dec 5 23:55 octave-bug-2.1.72
Dec 5 23:55 octave-bug -> octave-bug-2.1.72
Dec 5 23:55 octave-2.1.72
Dec 5 23:55 octave -> octave-2.1.72
Dec 5 23:55 mkoctfile-2.1.72
Dec 5 23:55 mkoctfile -> mkoctfile-2.1.72
Dec 5 23:55 ncgen
Dec 5 23:55 ncdump
Dec 5 23:55 blas-config
Dec 9 12:31 oneko
Dec 9 13:56 neko -> oneko
Dec 13 21:54 unrar
Jan 29 20:23 xdaliclock
eb 15 23:08 xsetroot
eb 15 23:11 oclock
eb 15 23:11 xconsole
eb 15 23:19 xcalc
eb 15 23:19 xbiff
eb 15 23:20 xset
eb 15 23:20 xman
eb 15 23:20 xeyes
eb 15 23:20 .
reenshot

Now


Activities
Thu 09:24
ilja van sprundel
Type to search...
LibreOffice Writer

Intro

- Initially had about a week or so of time to play around with this
- Made some interesting observations
  - Simple command line tools
  - Some code reading
- Found some clear problems
- Maybe a solution or two

What was actually done (observations)

- Started off with very simple commands to enumerate some entrypoints
- Wanted to see:
  - shared memory (and it's acl's) (ipcs)
  - Udp/tcp/unix sockets exposed locally (netstat –pln)
  - Look at cron scripts
  - …

What was actually done (observations)

- …
- Wanted to see:
  - Look for world writable files and directories
    - find / -perm -0666 -type f
  - Enumerate suid files
    - find / -perm +2000 -o -perm +4000 -type f
  - Enumerate dbus system endpoints
    - dbus-send --system --type=method_call --print-reply --dest=org.freedesktop.DBus /org/freedesktop/DBus org.freedesktop.DBus.ListNames

What was actually done (observations)

- Expected this to be pretty boring and coming up almost empty handed
- Varying results for various distro's and operating systems
- There seem to be some systemic issues across all of them
- Is no one doing trivial entrypoint analysis before shipping ?

Overall finds (problems)

- Without disclosing details (bugs aren't fixed)
  - world writeable shared memory
  - World writable scripts
  - Really really bloated suid binaries
  - misconfigurations
  - Over 60 finds in less than a week
- The goal of this talk isn't any specific bug

More observations

- Dbus
- Relatively new attack surface
- X/Gnome/KDE specific
- Ipc mechanism to pull information about the system or the current session
- Session is probably not that interesting
- System could be!

More observations

- Dbus
- Loads of new attack surface
  - Configuration
  - Design (repurposing)
  - Implementation (e.g. buffer overflow)
- There seem to be piles and piles of these installed on default linux distro's (40-60)

More observations

- Dbus system
- Configure who can read / write to it
  - Under what circumstances (root, console, group, default, …)
  - Where (what interface, …)
- /etc/dbus-1/*
- Xml-alike file that specifies this

More observations

- Have been configuration bugs here in the past:
  - http://pkgs.fedoraproject.org/cgit/sectool.git/tree/sectool-0.9.5-dbus.patch?id=aedb3ef7f7e5ab22d5438bfb7eee63489ccf3244;id2=4859832281f0e08c6fbe48fc252c4199a0e9e322

More observations

blob: aedb3ef7f7e5ab22d5438bfb7eee63489ccf3244 (plain)

```
diff -up sectool-0.9.5/org.fedoraproject.sectool.mechanism.conf.dbus sectool-0.9.5/org.fedoraproject.sectool.mechanism.conf
--- sectool-0.9.5/org.fedoraproject.sectool.mechanism.conf.dbus 2012-04-03 15:21:05.521186717 +0200
+++ sectool-0.9.5/org.fedoraproject.sectool.mechanism.conf      2012-04-03 15:23:57.602490428 +0200
@@ -9,7 +9,6 @@
       <allow own="org.fedoraproject.sectool.mechanism"/>
   </policy>
   <policy context="default">
-      <allow send_destination="org.fedoraproject.sectool.mechanism"/>
-      <allow send_type="method_call"/>
+      <allow send_destination="org.fedoraproject.sectool.mechanism" send_type="method_call"/>
   </policy>
 </busconfig>
```

More observations

- Easy to make config mistakes
- Similar to android intent permissions being set in their AndroidManifest.xml file

More observations

- I wanted to look a bit closer at the suids
- Asked readelf to give me a list of the library dependencies (readelf –d)
- All those libraries themselves are attack surface as well
- Some have just libc
- Others depends on huge blobs of network parsers (e.g. X).

More observations

```
ilja@ilja-VirtualBox:~$ readelf -d /usr/bin/kppp

Dynamic section at offset 0x82ec8 contains 33 entries:
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared library: [libkde3support.so.4]
 0x00000001 (NEEDED)                     Shared library: [libQt3Support.so.4]
 0x00000001 (NEEDED)                     Shared library: [libkio.so.5]
 0x00000001 (NEEDED)                     Shared library: [libkdeui.so.5]
 0x00000001 (NEEDED)                     Shared library: [libkdecore.so.5]
 0x00000001 (NEEDED)                     Shared library: [libQtCore.so.4]
 0x00000001 (NEEDED)                     Shared library: [libQtDBus.so.4]
 0x00000001 (NEEDED)                     Shared library: [libQtGui.so.4]
 0x00000001 (NEEDED)                     Shared library: [libstdc++.so.6]
 0x00000001 (NEEDED)                     Shared library: [libc.so.6]
…
```

More observations

File: /usr/games/gnomine

Dynamic section at offset 0x17ea4 contains 35 entries:

```
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared library: [libgtk-3.so.0]
 0x00000001 (NEEDED)                     Shared library: [libgdk-3.so.0]
 0x00000001 (NEEDED)                     Shared library: [libpangocairo-1.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [libpango-1.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [librsvg-2.so.2]
 0x00000001 (NEEDED)                     Shared library: [libgio-2.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [libgdk_pixbuf-2.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [libgobject-2.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [libglib-2.0.so.0]
 0x00000001 (NEEDED)                     Shared library: [libcairo.so.2]
 0x00000001 (NEEDED)                     Shared library: [libpthread.so.0]
 0x00000001 (NEEDED)                     Shared library: [libc.so.6]
…
```

More observations

- I spend some time zooming in on those using X
- X is a client/server protocol to be used for the gui in most unices
  - Including most linux distributions
- It's networked (can be tcp/ip, ipc, …)
  - Binary protocol
- In suids in question are basically clients
- You can make them connect to arbitrary X servers using the DISPLAY variable
  - Who says these have to be well behaving X servers ?

More observations

- The X client libraries (Xlib) are clear attack surface
- Spend about a day looking at the network parsing code in Xlib
- Things are ***really really*** bad
  - Binary protocol parsers in C.
  - Server data appears to be trusted. Very little validation
  - > 60 trivial bugs
- It's clear that code was written with no trust boundary in mind at all.

More observations

- The X client libraries (Xlib)
- All discovered X bugs are being fixed
- The developer involved is actually quite good
- And had some interesting comments

More observations

“I don't know how many setuid X clients still exist these days (is xterm still setuid on any platforms, or did they all get grantpt() or similar calls to avoid needing root?), but since we know there's more X clients than we can keep track of (especially once you get to home grown apps in various companies they've been using for decades), we have to assume there still may be some. It would be good to put a reminder in the security advisory that best practice is to separate out the parts of an application that require elevated privileges from the GUI to avoid such issues - GTK requires this, but not all toolkits do.”

More observations

"Shoot me now. And then shoot daniels for not freeing us from XKB yet. And then shoot anyone who volunteers to try to fix XKB, before it's too late for them too."

"Here's my initial analysis of the first part of the Xlib set, until I got so tired my head started spinning trying to figure them out"

"Really, if your window shape is anywhere near 2^32 rectangles, what are you doing?"

"Yes, these [bugs] all seem possible, and far more feasible now than when this code was written, back when disk sizes were still measured in megabytes."

More observations

- However, Raw X is rarely used nowadays
- There's stuff build on top
- And they use raw X
  - gtk+
  - KDE (which uses QT which uses raw X)
  - Rare direct calls to Xlib code
  - other

More observations

- KDE / QT
- Crappyness is about on par with Xlib
- Trivial bugs!

More observations

- Several instances of this

```
Qkeymapper_x11.cpp
void QKeyMapperPrivate::clearMappings()
{
...
        uchar *data = 0;
        if (XGetWindowProperty(X11->display, RootWindow(X11->display, 0), ATOM(_XKB_RULES_NAMES), 0, 1024,
                               false, XA_STRING, &type, &format, &nitems, &bytesAfter, &data) == Success
            && type == XA_STRING && format == 8 && nitems > 2) {
...
            char *names[5] = { 0, 0, 0, 0, 0 };
            char *p = reinterpret_cast<char *>(data), *end = p + nitems;
            int i = 0;
            do {
                names[i++] = p;
                p += qstrlen(p) + 1;
            } while (p < end);
...
}
```

More observations

- In QT init code (affects all QT applications)

```
Qapplication_x11.cpp
void qt_init(QApplicationPrivate *priv, int,
                Display *display, Qt::HANDLE visual, Qt::HANDLE colormap)
{
...
        } else if (arg == "-name") {
            if (++i < argc)
                appName = argv[i];  ← if it was previously new'ed, it isn't anymore.
        }
...
}


void qt_cleanup()
{
...
    if (X11->foreignDisplay) {
        delete [] (char *)appName;  ← could delete [] a pointer that isn't new'ed and possibly corrupt memory
        appName = 0;
    }
...
}
```

More observations

- So I reported this bug
- They didn’t not seem to think it was a security issues
- Quote from X developer (previous slide) is dead on
  - Suid remark
- QT does not seem to agree with this

More observations

- "KDE has precisely one setuid application, kcheckpass, for this reason. I suspect that someone running an suid Qt application would fall into a huge number of problems, the most obvious one being a malicious style that would allow them to trivially execute arbitrary code“

- Wait, did we just get a free Code exec bug from the QT security team ?

More observations

- I respond back, saying there are more KDE suid binaries, and specifically mention kppp, and question him on the styles thing

More observations

> I am aware of this, regardless, this is library code, as such, chances are, there are suid applications out there that will use it.

That would be a security hole in those applications rather than in Qt, there are many ways that people can abuse a library to create unsafe applications.

> Do styles contain executable code ?

Yes.

More observations

> also, does kppp no longer run suid ?

kppp should not be installed setuid. Here's a quote from its FAQ:

"There is no need for the setuid bit, if you know a bit of UNIX® systems administration. Simply create a modem group, add all users that you want to give access to the modem to that group and make the modem device read/writable for that group."

I doubt any modern distro would install it suid, in fact most are extremely careful about what they allow to be suid and are actively working to minimise what is.

More observations

- That kppp FAQ quote in incomplete, it goes on to say:

"… The KPPP team has lately done a lot of work to make KPPP setuid-safe. But it's up to you to decide if you install and how you install it."

More observations

- In fact, distro's do still have it suid.
- E.g. Ubuntu
- This is library code! They should not set policy for the apps that use them.
- They're sitting on the fence, because it's easy
  - you don't actually have to do anything
- Either defend it, and shut up
- Or do a suid check and exit()

More observations

- None of those bugs are fixed
- Got the ok from QT security team to disclose:

“> Ok, since you guys don't consider this a security issue, you're ok with me talking about this publicly?

Yes, that's fine”

More observations

- So loaders have LD_PRELOAD
- And has been made setuid safe years ago
- KDE/QT
  - QT_PLUGIN_PATH
- Gnome
  - GTK_MODULES
- Neither are setuid safe !

More observations

- The GTK+ people seem to be doing somewhat better.
- They do not allow suid GTK+ applications.
- And clearly explain why on their webpage

More observations (http://www.gtk.org/setuid.html)

The GTK+ Project

The GTK+ Project

About Features Download Screenshots Documentation Development

Why GTK_MODULES is not a security hole

GTK+ supports the environment variable `GTK_MODULES` which specifies arbitrary dynamic modules to be loaded and executed when GTK+ is initialized. It is somewhat similar to the `LD_PRELOAD` environment variable. However, this (and similar functionality such as specifying theme engines) is not disabled when running setuid or setgid. Is this a security hole? No. Writing setuid and setgid programs using GTK+ is bad idea and will never be supported by the GTK+ team.

You should not write setuid GTK+ programs because:

- GTK+ is too big. GTK+-1.2 and its dependent libraries (ignoring Xlib) total over 200,000 lines of code. For GTK+-2.0 (ignoring Xlib and image loading libraries), this figure will be around 500,000 lines of code.
- GTK+ is too complex. GTK+ takes input from dozens of sources, from drag-and-drop, to root-window properties, to keyboard input, to configuration files. This is a much broader scope for compromises than a typical server and makes auditing GTK+ especially tricky.
- Security of GTK+ requires the security of Xlib. The GTK+ team is not prepared to make that guarantee. Security bugs have been found in the recent past in such areas of Xlib as the input method code.
- You should not make your GUI setuid at all. Why run the risk of security bugs in code that does not need to be running with elevated privileges?

In the opinion of the GTK+ team, the only correct way to write a setuid program with a graphical user interface is to have a setuid backend that communicates with the non-setuid graphical user interface via a mechanism such as a pipe and that considers the input it receives to be untrusted.

For this reason, no effort is made in GTK+ to disable the obvious ways that you could compromise a setuid GTK+ program - GTK_MODULES and the ability for the user to specify theme engines, because we consider this to be only papering over the fundamental problems of writing setuid programs with *any* GUI toolkit. GTK+ may be modified in the future to simply refuse to run with elevated privileges, though it does not do this currently.

Does this mean that there are no security considerations for GTK+? No. In particular image loaders have been and will continue to be an area of special care, since users may load images from untrusted sources. And in addition to the possibility of this variety of exploit, most potential security holes are essentially bugs and even as mere bugs, must be squashed. To help accomplish this goal, GTK+ extensively uses high-level data structure abstractions which minimize the risk of most traditional buffer overflows.

However, the secure setuid program is a 500 line program that does only what it needs to, rather than a 500,000 line library whose essential task is user interfaces.

Copyright 2007-2008 The GTK+ Team

More observations

- This is beautiful, well though out and sane!
- "Security of GTK+ requires the security of Xlib. The GTK+ team is not prepared to make that guarantee"
- Or is it ?

More observations

Gtkmain.c

```
/* This checks to see if the process is running suid or sgid
 * at the current time. If so, we don't allow GTK+ to be initialized.
 * This is meant to be a mild check - we only error out if we
 * can prove the programmer is doing something wrong, not if
 * they could be doing something wrong. For this reason, we
 * don't use issetugid() on BSD or prctl (PR_GET_DUMPABLE).
 */
static gboolean
check_setugid (void)
```

More observations

- What does that mean ?
- Suid binaries can use GTK+, ***BUT*** …
- … they must acquire the privileged resources they want first
- And then then drop privileges
- After that it's ok to use GTK+
- Want to have their cake and eat it too
- Check should be stronger!

More observations

- games are a great example
- They are suid
  - Share a highscore database
- Once aquired, privs are dropped
- Only thing an attacker would have access to is that db
  - assuming a bug was found and exploited
- That db is considered trusted.
  - Any security bug in db parsing allows for further escalation
- Any user now playing any of those games gets pwned

More observations

- Spend a little bit of time looking at x display managers
- There's a lot of them
- Uses xdmcp protocol (goes over udp)
- Most have dependancy on libxdmcp for this
- Libxdmcp's api's quite easily lend themselves to abuse
  - Leaves a lot of stuff uninitialized on failure
- This is being fixed

More observations

- LightDM
  - Used by ubuntu
- Has so called greeters that allow you to customize the gui
- Unpriv'ed greeters talk to LightDM
  - Using a pipe
- Parser for that pipe wasn't great
  - Not that bad either
- Bugs are being fixed

More observations

- As mentioned earlier, libraries build on top of X use Xlib
- Apps will sometimes also call some X api's to query certain things
  - Using the XGetWindowProperty() api or any number of api's build on top of it (e.g. XGetClassHint(), XGetRGBColormaps(), …)
- Looked at the use of Xlib api's
- This too wasn't great

More observations

- By far the most common bug when using Xlib

```
void fn()
{
...
    SomeFormat *sf;
...
        (void) XGetWindowProperty(dpy, w, property, 0L,
                                  10000000, False, SomePropertyType, &type, &format,
                                  &length, &bytesafter, (unsigned char **) &sf);
...
       XFree((char*)sf);
...
}
```

- Check return values !

More observations

- Developers using Xlib don't seem to realize that most of the api's they use parse potentially untrusted network code
  - _XReply
  - _XRead32
  - _XRead
  - _XGetAsyncReply
  - XGetWindowProperty
  - XNextEvent
  - XPeekEventXIfEvent
  - XCheckIfEvent
  - XPeekIfEvent
  - XCheckTypedWindowEvent
  - XSetErrorHandler
  - XQueryFont

More observations

- derived from XGetWindowProperty:

- XFetchName
- XGetIconName
- XGetSizeHints
- XGetWMHints
- XGetWMSizeHints
- XGetIconSizes
- XGetTransientForHint
- XGetClassHint
- XGetRGBColormaps
- XGetTextProperty
- XGetWMName
- XGetWMIconName
- XGetWMClientMachine
- XGetCommand
- XGetWMColormapWindows
- XGetWMProtocols

- XScreenResourceString
- XFetchBuffer
- XFetchBytes
- XkbRF_GetNamesProp

More observations

- Conceptually there's a couple of X suid apps around that you'll see:
  - Config tools (e.g. kppp)
  - Games (e.g. swell foop)
  - Screen locking utils (e.g. Xlock, Xlockmore, Xscreensaver, …)
- Virtually all of these apps do drop privileges

More observations

- the screenlocking utils
- Only seem to capture your hashed pw entry (and optionally root).
  - Getspnam()
- W00t. That's not much of a resource
- Or is it ?

More observations

- The linux shadow library is responsible for api's for reading from and writing to the shadow file
- Shadow.h
- The code uses FILE stream api's to read and write
  - Uses heap buffers internally, Can't clear memory.
- Stores read data in local stack buffers
  - Doesn't clear memory
- Basically leaks the entire shadow file onto the heap and the stack

More problems summary

- Xlib in suids is a bad idea
- GTK+ kinda sorta still allowed in suids
- Very common sloppy misuse of Xlib api's
- Linux shadow library handles sensitive data in a sloppy manner

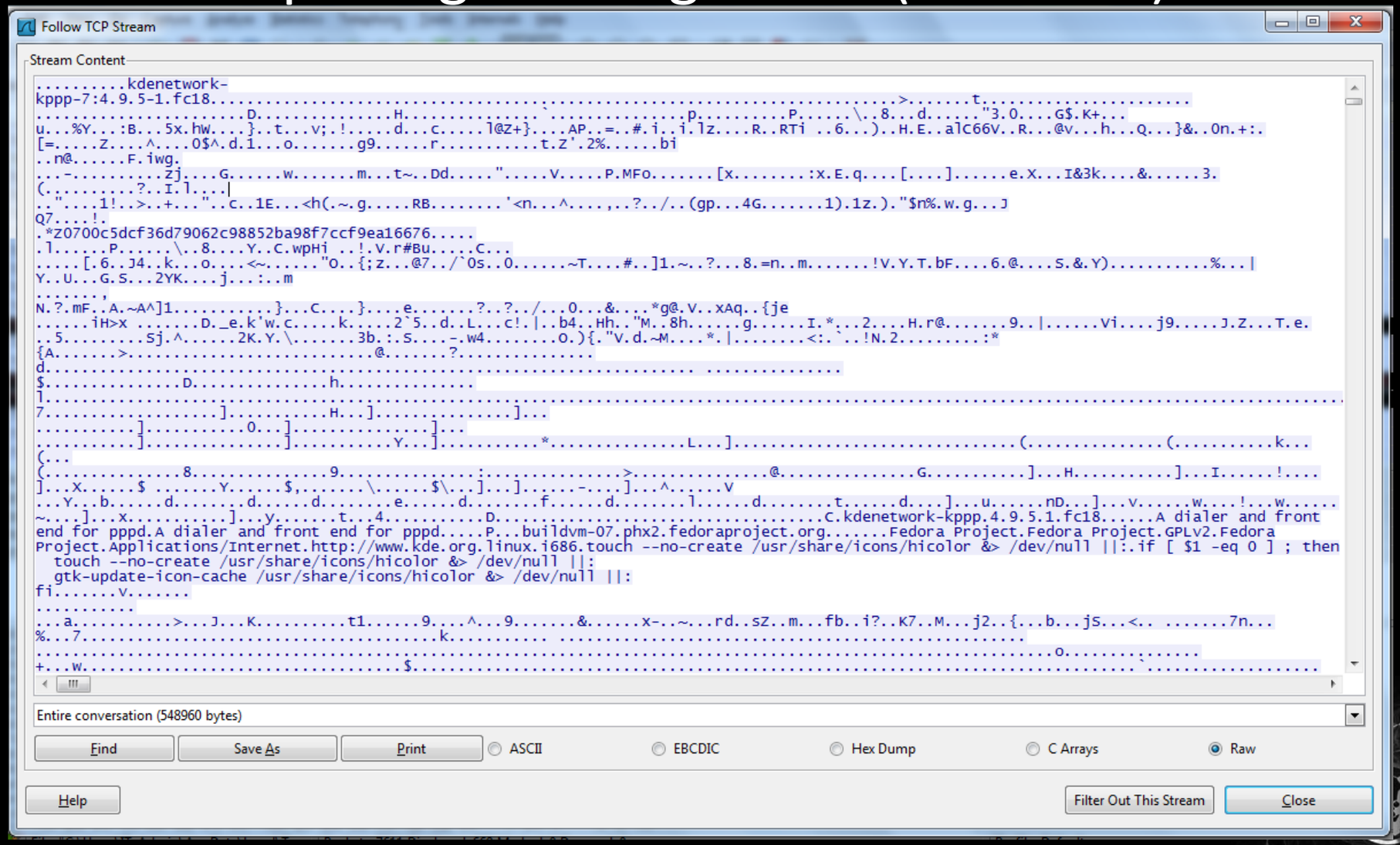
todo

- There's some other things we wanted to look at but didn't get around too
- Package managers
- Clipboard

- Ok, we did look for about 5 seconds
- It did look bad ….

todo

- Fedora package management (software)



todo

- Ubuntu apt-get

Follow TCP Stream

Stream Content

```
GET /ubuntu/pool/main/libd/libdbi/libdbi1_0.8.4-6_i386.deb HTTP/1.1
Host: be.archive.ubuntu.com
Connection: keep-alive
User-Agent: Debian APT-HTTP/1.3 (0.9.7.5ubuntu5)

HTTP/1.1 200 OK
Date: Thu, 07 Mar 2013 16:32:11 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Tue, 01 May 2012 00:07:17 GMT
ETag: "7500-4beee5a84f740"
Accept-Ranges: bytes
Content-Length: 29952
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-debian-package

!<arch>
debian-binary   1335815722  0     0     100644  4         `
2.0
control.tar.gz  1335815722  0     0     100644  1947      `
..........Z[s....k.+.d.vg"..(Qv.L.u..Lw.i......$@
5IO........,.$.>..vq&.e~...xn..w~.....W..7.......A.Z..j...p.^...#..
............+..+.z:./....p..W........<..<f.\n.I..Q.9z../.b......P..."...7Tns.K......7.3.
=Kx..L.....OHmi..!'.U'e..}I...+i../..+O..rW.<._....` .........6..C .I.\.]...}....?.........D.&.......7....s7n..ii.e.+.%
[,d.e....yD.."....Tty..M#..U..]\..IP.A.)#..@!....~.....8E).912.o...$...#p.
^DR.VfX....C..J]4v.<J.."..<.....\../.(....l........j....g...<.g...,>.r.}..<X..........C5.m.9E...pt.!
r...X?.K=..O.XD....8C.Q....~@....}.F....#9.....7>.}...
.........AU.W$.rHW....a.)K........9....8..n
..|dv{..;.,..I..P.......*.]?.+:O.jp...>...}..C.W......s.O(...f...y.1.I...."z.....x..y.@)....e*.r$O.x.=...b.....m'..x..m..k..n%./*.Sb
$B.....G......&N.aq..{...kL.....*>{
.M....Dw\.N.7..Xo&.1c..p..fO..MX..(.e...V2..K....q .I.R...o.1.^v...K...k(.FJ...C.9VF.....y.....
$...<.@@t)......c...3......./...v.......H.#....T..|. .`..u.."......h&...#,....Q..o!....gw.OLi}........1=mt....x..N9.8M.
$...Lm........4..S..Q....X....aj....8.....4.j.=>E..=St....%
A.O.D8Ma...d<.....Of..e>OF...m..c,=V.....G.MO.6=.&zJ..)...F..u...........kN%...S.....1..KJozq....\2.
N.....nG......n.....4.z.o..So...?./......O..?......?6O.o../[J............_.m.?.|..
...!.?q-.....m'.j..l.....)XUk.,........^....T.].[..
nF/usiF.K3.d..|S.c)..r.^.v.&XVoP............\.......Bc.K.........9%.O..w.|.w.iEK".9$k...wh...9...7.e\.dK....Y......A....
+.....|....C .b.8`/.....AU6......s>..]....QO.`.t....q.....j..U........
[R.3uK..O..7.W....P.f..T.m..........@p#...fH.Z..zx........i..J...
..r..#..Hg..d%.....`9d..N}..L.O.~w...HE.._`....xIQF.z...'.x..../P%x&pQ.!...,.x..$.....m@.`!.....`O...2...qI..........m}.I....e..O
(....u.....V.I..c=..3s...._.............."X....B.x....?N..OH.^/.e.Y..8!A. WD]..G'.
\.....Y..e...2...4].tIVxE..2l.lrgNx........On...`.L)............& I...?t...e..%s..>..p|...%....A...e......B._...x....U..eo
{.w._...|.78?...K.............b...+V.X.b...+V.X.b...+V.X.b...+V.J...]...P..
data.tar.gz     1335815722  0     0     100644  27811     `
```

Entire conversation (271127 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

todo

- OpenSuse zypper

Follow TCP Stream

Stream Content

```
GET /distribution/12.2/repo/oss/suse/i586/rrdtool-1.4.7-4.1.2.i586.rpm HTTP/1.1
User-Agent: ZYpp 11.6.2 (curl 7.25.0) openSUSE-12.2-i586
Host: download.opensuse.org
X-ZYpp-AnonymousId: 222b313d-28bf-4d67-a6ea-fcbefb1eebc1
X-ZYpp-DistributionFlavor: dvd
Accept: */*, application/metalink+xml, application/metalink4+xml

HTTP/1.1 200 OK
Date: Fri, 08 Mar 2013 00:09:00 GMT
Server: Apache/2.2.12 (Linux/SUSE)
X-Prefix: 208.181.206.0/23
X-AS: 852
Vary: accept
Content-Disposition: attachment; filename="rrdtool-1.4.7-4.1.2.i586.rpm.meta4"
Transfer-Encoding: chunked
Content-Type: application/metalink4+xml; charset=UTF-8

1f89
<?xml version="1.0" encoding="UTF-8"?>
<metalink xmlns="urn:ietf:params:xml:ns:metalink">
  <generator>MirrorBrain/2.15.0</generator>
  <origin dynamic="true">http://download.opensuse.org/distribution/12.2/repo/oss/suse/i586/rrdtool-1.4.7-4.1.2.i586.rpm.meta4</origin>
  <published>2013-03-08T00:09:00Z</published>
  <publisher>
    <name>openSUSE</name>
    <url>http://download.opensuse.org</url>
  </publisher>

  <file name="rrdtool-1.4.7-4.1.2.i586.rpm">
    <size>616657</size>
```

Entire conversation (16111 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

todo

- Lets hope they sign stuff
- And check it
  - And have signatures locally
  - Or fetch them securely from a remote host
- And don’t use md5 …
- Even if you’ve got all this correct
- Network protocol is unencrypted
- Adds a lot of remote attack surface

todo

- Clipboard
- ICCCM
- It smells rotten
- http://lists.slug.org.au/archives/slug-chat/2001/July/msg00054.html
  - Srsly, go read it
  - No, really!
  - It’s all I know about ICCCM, but it speaks volumes

todo

“d00d, that document is devilspawn…. what sick evil twisted mind wrote this damn spec?”

“The ICCCM is the coding equivalent of the Medieval rack, except its advertised as some kind of X11 swingers party.”

“I've seen more elegant protocols in unlikely places. When blowflies fight over a pile of elephant shit, their pecking order is a more elegant protocol than ICCCM.”

“I. C. C. C. M.

Inter-
Client
Communications
Conventions
Manual!

Manual, like in "manual labour", like in "pain"
Conventions, like in "not required, just do ALL OF IT or you SUCK!"
Communications, like in "fucking overengineered carrier pigeons"
Client, like in "see that guy with the limp, he was one of my ``clients''"
Inter-, like in "Inter-nal bleeding“”

Solutions ?

- The shadow library thing is easy to fix
- It's not really a bug in the first place
  - But exposes too much sensitive information to an already compromised suid program
- Drop all FILE stream usage.
  - Use open/read/write syscalls instead
- Clear all memory after use
  - Make sure memset() doesn't get optimized out by compiler

Solutions ?

- Most suids on linux (and most unices) have been dropping privileges for a long time
  - Nothing has changed since
- This isn't good enough.
- Those privileged resources include:
  - read fd to /dev/kmem
  - read/write fd to /etc/resolv.conf
  - Full content of /etc/shadow
  - …

Solutions ?

- The suid processes still have their suid bit set in kernel
- Attacker still needs some kind of bug + exploit
- reduced what can be gained from uid 0 to those resources
  - Is however still very significant

Solutions ?

- A model where priv dropping and priv separation is combined would make more sense
- Would add more defense in depth
- Probably not that hard to implement for some suids

Solutions ?

- Here's what it would looks like:
  - pipe
  - fork
  - client drops all privs
  - server gets resources
  - server drops privs
  - very small and well defined interface between client and server

Solutions ?

- Client retains it's suid bit
  - Pipe to server is protected from injection
- readelf –d on some of the suids
  - HUGE list of library dependencies!
- We don't want that in service code.
- fork() is out!
  - If you fork, all that stuff is still in memory.

Solutions ?

- fork() is out, fork() + execve() is in.
- Pass fd to excve'ed process.
- Server has to be a very small piece of c code.
- Only access to libc.

Solutions ?

- Actually, glibc (default on most distributions) is super bloated.
- > 100mb of source code (2.1.7)
- Can you really trust that ?
- Should not be used in server app
- Instead use somethine like dietlibc or uClibc

Solutions ?

- One last piece of code bloat left
- Dynamic loader.
- Takes input though environment variables
- Have been bugs in there in the past
- Do you really want to trust it ?
- Fix: static binaries

Conclusion?

- Guess there should be a conclusion
- Run for the hills ?
- Things could be better …
- … by several orders of magnitude

- There's really a lot of work here
  - most of that code is not written with a trust boundary in mind

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Questions ?