Subject: Re: TinyVZ 0.7 released
Posted by Solar Designer on Mon, 22 Aug 2011 20:44:52 GMT
View Forum Message <> Reply to Message

On Mon, Aug 22, 2011 at 02:35:35PM -0400, Sam Trenholme wrote:
> You know, this is going to make me start yet another almost completely
> off-topic rant.

I like and agree with most of what you wrote.

> One of the reasons I have kept the number of packages in my TinyVZ
> distribution down to an absolute minimum is because this minimizes the
> number of potential security holes I will have to babysit in this
> distribution.

Sure. We do the same thing in Owl - e.g., trying to avoid having more than one implementation of a feature. I think we may start to deviate from this soon, though, due to popular demand... Saying that we don't have wget in the base system because we have lftp (which has a mirror command, ftp/http/https, and includes lftpget) doesn't always cut it.

> > Does uClibc ensure that fd 0-2 are open on program startup (opening them to
> > /dev/null / /dev/full if not)? I doubt it. I admit I haven't checked,
> > though.
>
> It might. It might now. I haven't checked either. What I can tell
> you is that there does not appear to be any vulnerability reports for
> uClibc:
>
> http://security-tracker.debian.org/tracker/source-package/uc libc

This could mean no security issues, or more likely it could mean that no one cares about "local" security issues, or that upstream does not care about such issues even if some users do. I don't know which it is.

As to musl, I brought the fd 0-2 issue up and as expected Rich is going to fix it:

http://www.openwall.com/lists/musl/2011/08/22/5

> > I think a better libc to use for this purpose would be musl:
> >
> > http://www.etalabs.net/musl/
> >
> > It also lacks some of those highly desirable security measures, but I
> > think it will gain those soon.
>
> If I were to do this again in a few months, I may use musl; however

> musl is an "alpha" product while uClibc is a mature product that is
> still being updated. I use the code which works today; that's why I'm
> using OpenVZ and not, say, LXC [2].

This makes sense.

musl might actually be more mature than LXC, though, if these can be compared at all (apples and oranges, indeed). There's already an experimental desktop distro with X built upon musl.

> TinyVZ is, in truth, me putting closure on a project I had back in
> 2007 (around the time I started rewriting MaraDNS's recusrive
> resolver) making a tiny uClibc + Busybox live CD distribution for
> having on a business card CD so I could use cyber cafes and friends'
> infected computers in a reasonably secure manner.

Hmm, we already had Owl LiveCDs at the time (and much earlier), so you could just use that. ;-) Not for business card sized CDs (for full CDs), but you could either use a business card sized DVD (which works faster anyway) or exclude /usr/src and a few other optional things.

> > Meanwhile, the sad truth may be that under Linux we need to use (e)glibc
> > (or other clones of it) for SUIDs/SGIDs.
>
> This can very well be true.

I expect that musl will also be a valid option for this very soon.

> One thing I have done is minimize the
> attack surface with SUIDs by having only two SUID programs in the
> system: "passwd" and "su". While Busybox is supposed to have a way of
> having it be SUID and drop privileges as needed, I don't fully trust
> that mechanism; better to compile Busybox twice.

Sounds good. As you might have heard, we have no SUIDs in a default install of Owl (only some SGIDs). And, by the way, musl supports Owl's /etc/tcb shadowing scheme, so you can mix these two and have non-SUID passwd command in a tiny distro without PAM.

> With the full self-hosting development tree being just over 40 megs xz
> compressed, and a usable "DNS toaster" system (which is resolving all
> of my DNS queries as I type this) being about 2 megs in size, I think
> TinyVZ targets those who want to have a really small OpenVZ system.
> OpenVZ's strength is that it allows a single computer to safely run a
> dozen or more separate services with full compartmentalization. By
> making the containers as small as possible, I can visualize a single
> server rack with a hub inside of it, as well as a dozen or so
> credit-card sized computers with Atom SOC cpus, 4 gigs of memory, and

> 64GB SSDs. Each one of those computers can run dozens of really tiny
> OpenVZ single-task containers.

Sure. What you did is very nice.

For now, we're just using OpenVZ containers with instances of Owl, though.
That's 112 megs under .tar.gz, not 40, but it is still acceptable for
systems with disks.

> Owl looks like a really good distribution, and I think it is very wise
> to stay in step with RedHat, since then RedHat's security updates can
> be applied. Does OWL have its own mechanism for applying security
> patches, or does it just use the patches from CentOS or Scientific
> Linux [3]?

For stuff that is part of Owl (such as everything in our ISOs), we're
preparing and making available security and other updates ourselves:

http://openwall.info/wiki/Owl/upgrade

Indeed, we sometimes reuse patches prepared by other distro vendors (and
they sometimes reuse ours).

For stuff that a user/admin of Owl might install on top of Owl from
another distro's repository, indeed they need to use that distro's updates.

Alexander
