[liberationtech] Deterministic builds and software trust [was: Help test Tor Browser!]

Eugen Leitl eugen at leitl.org
Wed Jun 19 02:36:09 PDT 2013

- Previous message: [liberationtech] Deterministic builds and software trust
- Next message: [liberationtech] Deterministic builds and software trust [was: Help test Tor Browser!]
- **Messages sorted by:** [date] [thread] [subject] [author]

----- Forwarded message from Mike Perry <mikeperry at torproject.org> -----

Date: Tue, 18 Jun 2013 20:54:30 -0700
From: Mike Perry <mikeperry at torproject.org>
To: liberationtech <liberationtech at lists.stanford.edu>
Subject: [liberationtech] Deterministic builds and software trust [was: Help test Tor Browser!]
Reply-To: liberationtech <liberationtech at lists.stanford.edu>

Jacob Appelbaum:
> *Hi,*
>
> *I'm really excited to say that Tor Browser has had some really important*
> *changes. Mike Perry has really outdone himself - from deterministic*
> *builds that allow us to verify that he is honest to actually having*
> *serious usability improvements.*

First, thanks for the praise, Jake!

But: I've been meaning to clarify this "honesty" point for a few days
now, and Cooper's similar statement in another thread about security
being all about trust reminded me of it.

I actually disagree with the underlying assumptions of both points.

I didn't spend six agonizing weeks (and counting) getting deterministic
builds to work for Tor Browser to prove that I was honest or
trustworthy. I did it because I don't believe that software development
models based on single party trust can actually be secure against
serious adversaries anymore, given the current trends in computer
security and "cyberwar".

For the past several years, we've been seeing a steady increase in the

weaponization, stockpiling, and the use of exploits by multiple governments, and by multiple *areas* of multiple governments. This includes weaponized exploits specifically designed to "bridge the air gap", by attacking software/hardware USB stacks, disconnected Bluetooth interfaces, disconnected Wifi interfaces, etc. Even if these exploits themselves don't leak (ha!), the fact that they are known to exist means that other parties can begin looking for them.

In this brave new world, without the benefit of anonymity to protect oneself from such targeted attacks, I don't believe it is possible to keep a software-based GPG key secure anymore, nor do I believe it is possible to keep even an offline build machine secure from malware injection anymore, especially against the types of adversaries that Tor has to contend with.

This means that software development has to evolve beyond the simple models of "Trust my gpg-signed apt archive from my trusted build machine", or even projects like Debian going to end up distributing state-sponsored malware in short order.

This is where deterministic builds come in: any individual can use our anonymity network to download our source code, verify it against public signed, audited, and mirrored git repositories, and reproduce our builds exactly, without being subject to such targeted attacks. If they notice any differences, they can alert the public builders/signers, hopefully using a pseudonym or our anonymous trac account.

This also will eventually allow us to create a number of auxiliary authentication mechanisms for our packages, beyond just trusting the offline build machine and the gpg key integrity.

I believe it is important for Tor to set an example on this point, and I hope that the Linux distributions will follow in making deterministic packaging the norm. (Don't despair: it probably won't take 6 weeks per package. Firefox is just a bitch).

Otherwise, I really don't think we'll have working computers left in 5-10 years from now :/.

I hope to write a longer blog post about this topic on the Tor Blog in the next couple weeks, discussing the dangers of exploit weaponization and the threats it poses to software engineering and software distribution. I'm still mulling over the exact focus and if I should split the two ideas apart, or combine them into one post...

Ideas and comments welcome!

--
Mike Perry

----- End forwarded message -----
--
Eugen* Leitl leitl http://leitl.org

```
_____________________________________________________________
ICBM: 48.07100, 11.36820 http://ativel.com http://postbiota.org
AC894EC5: 38A5 5F46 A4FF 59B8 336B  47EE F46E 3489 AC89 4EC5
```

- Previous message: [liberationtech] Deterministic builds and software trust
- Next message: [liberationtech] Deterministic builds and software trust [was: Help test Tor Browser!]
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the liberationtech mailing list