SSL in FreeBSD

State of **LibreSSL** (and Open**SSL**)
In FreeBSD ports and base

Bernard (Barnerd) Spil
2016-01-31
FOSDEM 2016 BSD track

Introduction

- FreeBSD user since 5.4 (ca. 2005)
- NB: Not a developer, not a cryptographer, …
- Active contributor on the #freebsd channel
- Maintainer of LibreSSL ports (and MariaDB)
- Author of collection of **LibreSSL** ports patches
- Day job: EAI Architect at **PHILIPS** Lighting
- Volunteer at **HSLnet** (local FttH cooperative) and for Bits of Freedom (Privacy Café & Toolbox)

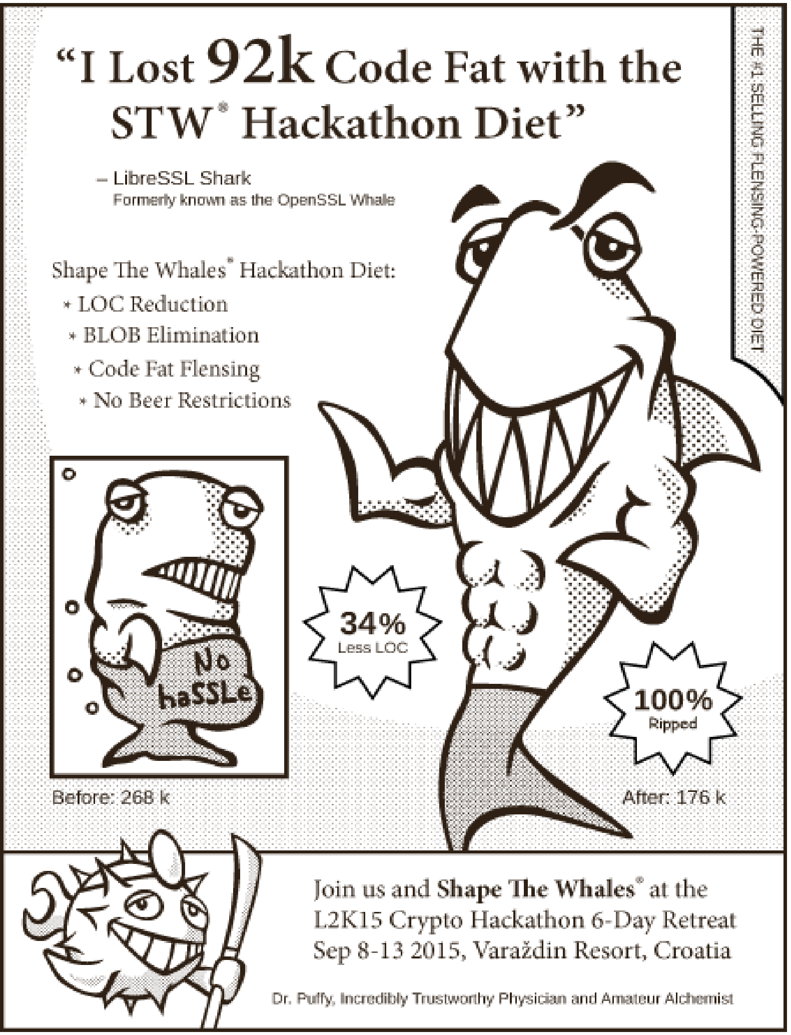
How did we get here

- We all recall Heartbleed[1]?
- April 2014 OpenBSD forks OpenSSL[2]
- **LibreSSL** liveblogs the sourcecode culling "OpenSSL Valhalla Rampage"[3]
- Support for old platforms is removed (Win16, OS/2, BeOS, VMS, etc.)
- Old, insecure features are removed (Export ciphers, compression, SSLv2, etc)

Core Infrastructure Initiative[4]

- Formed by the Linux Foundation after Heartbleed was discovered
- Commissions a security audit of OpenSSL by NCC Group
- Discovers numerous problems with the code
  - Fixed for the issues released by subsequent patch-releases of OpenSSL
  - Forcing frequent (emergency) patching for everyone

Where did **LibreSSL** end up?



"I Lost 92k Code Fat with the STW* Hackathon Diet"

– LibreSSL Shark
Formerly known as the OpenSSL Whale

Shape The Whales* Hackathon Diet:

- LOC Reduction
- BLOB Elimination
- Code Fat Flensing
- No Beer Restrictions

Before: 268 k

After: 176 k

Join us and Shape The Whales* at the
L2K15 Crypto Hackathon 6-Day Retreat
Sep 8-13 2015, Varaždin Resort, Croatia

Dr. Puffy, Incredibly Trustworthy Physician and Amateur Alchemist

- New codebase ca 35% smaller (incl new libtls!)
- ***LibreSSL***-portable first release 2.0.0 on 2015-07-11
- Further removal of features
- Addition of new libtls

PCBSD OPNsense

VOID openelec embedded linux entertainment center

So what about FreeBSD ?

- Frequent updates to OpenSSL in base

FreeBSD-SA-14:03
FreeBSD-SA-14:06
FreeBSD-SA-14:09
FreeBSD-SA-14:10
FreeBSD-SA-14:14
FreeBSD-SA-14:18
FreeBSD-SA-14:23

FreeBSD-SA-15:01
FreeBSD-SA-15:06
FreeBSD-SA-15:12
FreeBSD-SA-15:26

FreeBSD-SA-16:11

- security/libressl ported within a day
- Currently 2.2.6 and 2.3.2 (security/libressl-devel)

Vulnerabilities?

	LibreSSL	OpenSSL	LibreSSL	OpenSSL
	vs 1.0.1		vs 1.0.2	
Critical	0	0	0	0
High	0	4	0	2
Medium	14	25	12	17
Low	4	11	3	6
Total	**18**	**40**	**15**	**25**

NB: Yes, I know this is a stupid metric

That simple?

- With the first release a lot of packages fail to build or run (ca 100 out of 25k)
  - Including major projects like Apache httpd, Python, OpenLDAP, cURL, …
- Then came 2.3 without SSLv3 and SHA-0
  - Again ca. 100 packages fail to build
  - Again including major projects like Apache httpd, Squid, haproxy, Python, Ruby, cURL

The Perl
Entropy Gathering Daemon

- Back in the day, there was no /dev/random
- No current platform needs it yet projects are rife with RAND_egd (as of ca. 2004)

```
else if (pRandSeed->nSrc == SSL_RSSRC_EGD) {
   /*
    * seed in contents provided by the external
    * Entropy Gathering Daemon (EGD)
    */
   if ((n = RAND_egd(pRandSeed->cpPath)) == -1)
      continue;
      nDone += n;
}
```

(Apache 2.4.8)

Promises, promises...

- **2001**-10-24: “the OpenSSL DES functions are renamed to begin with DES_ instead of des_. Compatibility routines are provided and declared by including openssl/des_old.h.
The compatibility functions will be removed in some future release, **at the latest in version 1.0.”**

```
 static void
-des_ecb_encrypt( des_data_block *plain, des_data_block *encrypted,
-         des_context ctxt, int op)
+DES_ecb_encrypt( DES_data_block *plain, DES_data_block *encrypted,
+         DES_context ctxt, int op)
 {

- des_ecb_encrypt( &StdText, &PasswordHash2, schedule , DES_ENCRYPT );
+ DES_ecb_encrypt( &StdText, &PasswordHash2, &schedule , DES_ENCRYPT );
```

(OpenLDAP 2.4)

Bad examples

- Bad examples apparently propagate

  I haven't tried to find the root of this but there are consistent troublesome ways to use the OpenSSL API
- Makes patching easier…
- Please use the SSLv23 methods (or their TLS replacements) and SSL_OP_*
- Past week? Built -nossl2 yet SSLv2 ciphers are still usable (“Low” vuln CVE-2015-3197)

Upstreaming

- The larger and more active projects are mostly very happy to include fixes.
- There are many abandoned, dormant, etc. projects out there! Patching all fall-out at times felt like trawling through a morgue...
- Still a large number of fixes to upstream
- Check the FreeBSD wiki[7,8]

Additional OpenSSL issues

- Packages not honoring WITH_OPENSSL_PORT
  - Linking against base libssl/libcrypto instead
- Packages not specifying USE_OPENSSL
  - Yet linking against libssl/libcrypto
- Mix of Base and Ports OpenSSL causes issues (you ***must*** rebuild all ports when enabling WITH_OPENSSL_PORT)
- Fixing a typo in an ifdef “!!” to “||” in code never used

The past week

- You're here? No emergency patching all servers again?
- But seriously…
- One vulnerability classified “high”, one “low”.
  - SSLv2 ciphers still usable even when disabled…
- **LibreSSL** not affected, release prevents foot-shooting by forcing SSL_OP_SINGLE_DH_USE

Versions

FreeBSD version	OpenSSL version	Supported
9.x	0.9.8	EoL 2015-12-31
10.x	1.0.1	Security patches 2016-12-31
11	1.0.2	Full 2019-12-31

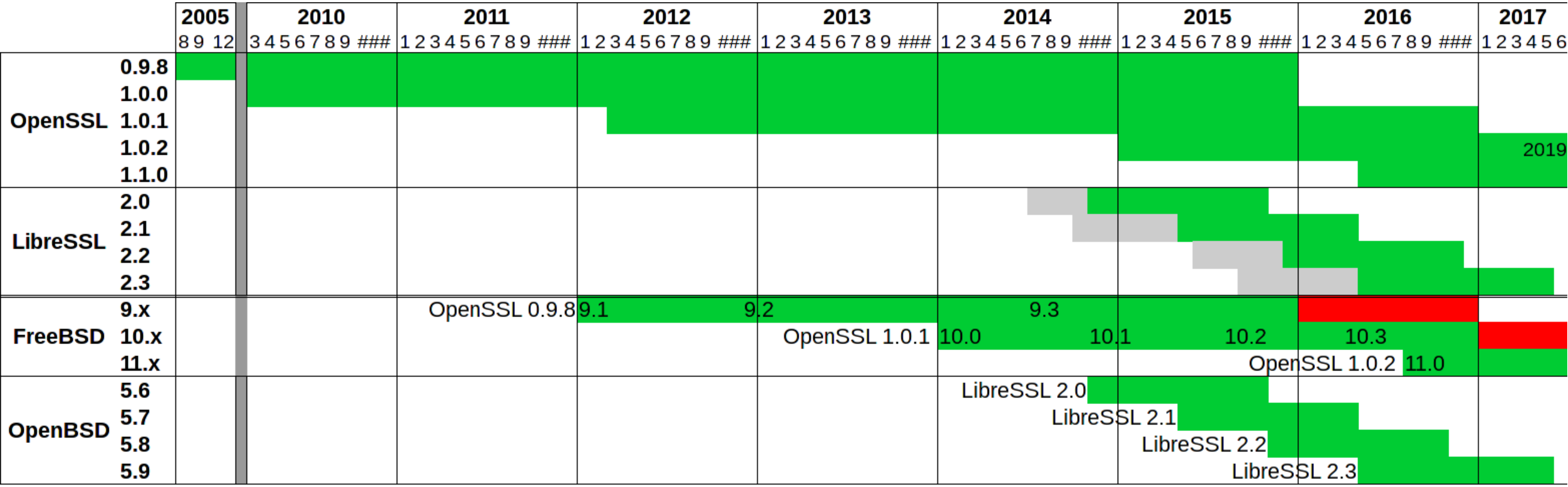
Most software is running with an outdated OpenSSL stack

OpenBSD version	LibreSSL version	Supported
5.7	2.1	2016-05-01
5.8	2.2	2016-11-01
5.9	2.3	2017-05-01

Release every 6 months, supported 1 year

Lifecycle

- FreeBSD major versions have too long a lifespan to keep up with SSL versions



Building FreeBSD without OpenSSL libs

- Thanks to Adam McDougall
- WITHOUT_OPENSSL=yes in /etc/src.conf is not a complete solution
  - WITHOUT_LDNS, WITHOUT_LDNS_UTILS
  - WITHOUT_PKGBOOTSTRAP
  - WITHOUT_SVNLITE
  - Patch to disable ctld, iscsid, bsdinstall and ssl in libfetch (ouch!)
- Only really useful for a package building jail

Making base SSL libs private

- FreeBSD base build framework can make libraries "private"
- 10.x: Moves these libraries to /usr/lib/private
- 11: Renames the library with libprivate prefix
- Ports can't 'find' the private libs and will fail or link against the libraries provided by ports
- Why? Not all ports use the correct libraries (see https://bugs.freebsd.org/195796 for a list)

Build using CURRENT

- Patch /usr/src
  - PRIVATELIB=true for libssl and libcrypto
  - Move libssl and libcrypto to _PRIVATELIBS
  - Small changes to kerberos and rescue
  - Add non-private libs to ObsoleteFiles
- Latest patch from Allan Jude available via FreeBSD wiki[5]

Result

- None of the files that originally linked against libssl or libcrypto still do
- E.g. /usr/bin/svnlite links to the private ssl and crypto.so
- All seems well
- Now that was simple…

Building on 10.2

- Make libssl and libcrypto private libs
  - share/mk and secure/lib/lib{crypto,ssl}/Makefile secure/usr.bin/openssl/Makefile
-
  ```
  libssl.so.7 => /usr/lib/private/libssl.so.7
  libcrypto.so.7 => /usr/lib/private/libcrypto.so.7
  ```
- Patch Makefiles

  ```
  USEPRIVATELIB= ssl crypto
  ```

  Applied to base binaries (pkg, libfetch, fetch, svn) works as well
- Latest patch-set available via FreeBSD wiki[5]

What's next

- Validate that this works properly
- ports-mgmt/pkg works with minor patches but introduces a circular dependency. Must find a way to link it to private ssl libs, initial patch from Allan Jude available.
- Use private libs to build all ports (looks like PC-BSD is up for it!)

Thanks

- OpenBSD (Bob, Joel, Theo, Brent, ...)
- Kris Moore from PCBSD for providing the build resources to repeatedly rebuild 10k ports
- 'frogs' from IRC for pushing me to get it done
- Allan Jude for the original work on Making SSL libs private in base.
- Vsevolod, Kubilay, Johannes and many more from the FreeBSD project for their invaluable help and guidance.

References/links

1) http://heartbleed.com/
2) http://www.tedunangst.com/flak/post/origins-of-libressl
3) http://opensslrampage.org/
4) https://www.coreinfrastructure.org/
5) https://wiki.freebsd.org/OpenSSL/Base
6) https://wiki.freebsd.org/LibreSSL
7) https://wiki.freebsd.org/OpenSSL/No-SSLv3
8) https://wiki.freebsd.org/LibreSSL/Ports
9) http://www.libressl.org
10) https://github.com/libressl-portable