The security of crypto in Red Hat Enterprise Linux

Dr. Nikos Mavrogiannopoulos
nmav@redhat.com

Red Hat, Inc.
May 2017
Overview

RHEL crypto engineering

- Who we are
- Crypto base
- Challenges we face
  - What we do for you via RHEL
Crypto engineering
Crypto engineering
Crypto engineering
Crypto engineering

Applications (glibc, rpm, httpd, …)

Language bindings

Protocols (TLS, SSH, Kerberos, IPSec, …)

Cryptography (RSA, ECDSA, AES, …)
Crypto engineering
Crypto engineering
RHEL today
RHEL today: crypto stacks

- OpenSSL
- GnuTLS
- NSS
- libgcrypt
- nettle
Challenge: Crypto has lifetime
Crypto has lifetime
Crypto has lifetime

- SHA-1 collision (2017)
- DROWN - SSL 2.0 (2016)
- SLOTH - MD5 (2016)
- Sweet32 - 3DES (2016)
- FREAK - EXPORT (2015)
- LOGJAM - 512b DH (2015)
- POODLE - SSL 3.0 (2014)
- RC4 (several weaknesses)
Crypto has lifetime: deprecation
Crypto has lifetime: deprecation
Crypto has lifetime: PCI-DSS
Crypto has lifetime: PCI-DSS

No legacy versions of TLS
Crypto has lifetime: PCI-DSS

No legacy versions of TLS

RHEL6.9: TLS 1.2

RHEL7.0: TLS 1.2
Crypto has lifetime: FIPS140-2
Policy enforcement

Applications

FIPS140-2

OpenSSL  NSS  OpenSSH  GnuTLS  libgcrypt

nettle
Policy enforcement

Applications

OpenSSL  NSS  GnuTLS  libgcrypt

nettle
Challenge: Implementation bugs
Implementation bugs

Heartbleed (2014)
Testing & Fuzzing

- OpenSSL
- NSS
- OpenSSH
- GnuTLS
- libgcrypt

- nettle
Testing & Fuzzing

OS integration (downstream)

OpenSSL  NSS  OpenSSH  GnuTLS  libgcrypt

nettle
Testing & Fuzzing

Test coverage (upstream)

OS integration (downstream)

OpenSSL  NSS  OpenSSH  GnuTLS  libgcrypt

nettles
Hardware Security Modules
Hardware Security Modules
Hardware Security Modules
Hardware Security Modules
Hardware Security Modules

OS

httpd
Hardware Security Modules
Hardware Security Modules
Hardware Security Modules
Hardware Security Modules

- Not a new idea; cheaper to use today
Hardware Security Modules

- Not a new idea; cheaper to use today
- Becomes easier to use, even on the cloud
Hardware Security Modules

- Not a new idea; cheaper to use today
- Becomes easier to use, even on the cloud
- Standardized API for applications (PKCS#11)
Hardware Security Modules

- OpenSSL engines
  - Apache HTTPD
  - Nginx
  - Openssl
- PKCS#11
  - Mod_nss
  - NSS
  - GnuTLS
Smart cards
Smart cards

Applications

PC/SC API

PCSC-lite

CCID
Smart cards

Applications

PKCS#11 API

Coolkey / OpenSC

PC/SC API

PCSC-lite

CCID
Smart cards

- CCID
- PCSC-lite
- PKCS#11 API
- PC/SC API

Applications

- Coolkey / OpenSC
- OpenSSL
- NSS
- GnuTLS
- OpenSSH
RHEL Present-Future
RHEL Present

- Solid crypto base, standards compliance
- HSM support (inconsistent)
RHEL Future

- Solid crypto base, standards compliance and consistent crypto policy

- Simple and consistent HSM support
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews

#redhat #rhsummit
Questions?

nmav@redhat.com
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews

#redhat #rhsummit