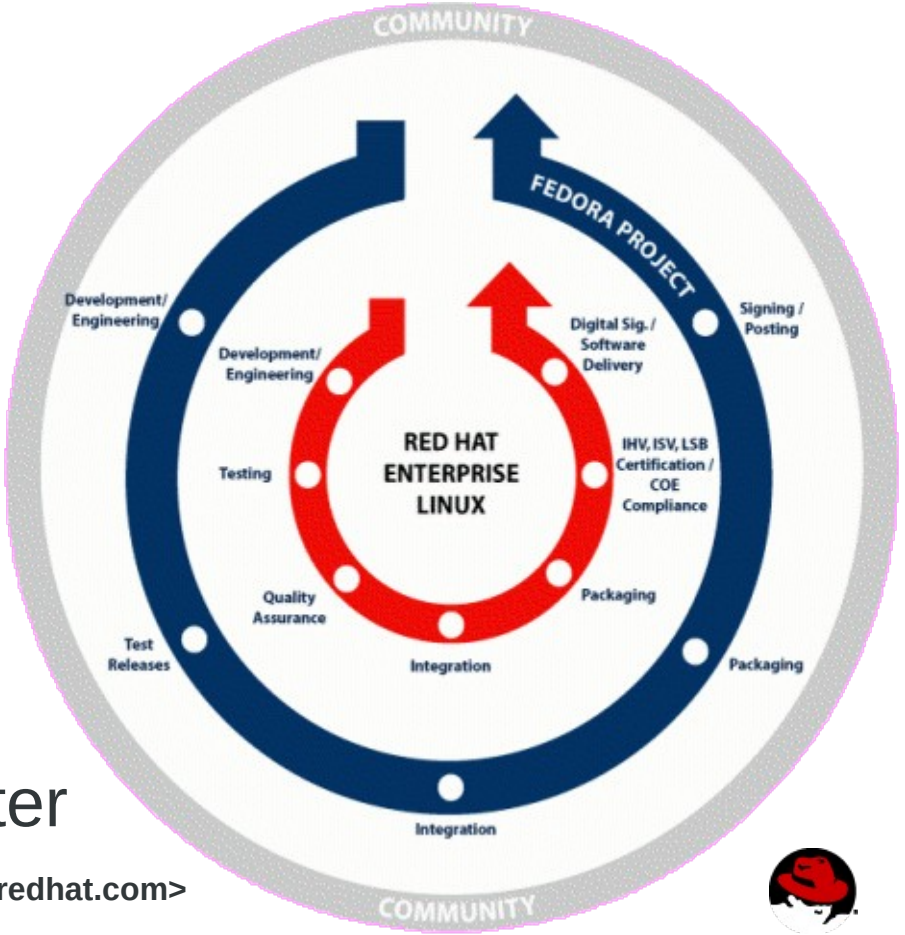
OS integrating of DNSSEC

Paul Wouters
Senior software engineer,
Red Hat
October 17, 2012

Red Hat Development Model

- Community driven – foster relationships with upstream
- Fedora Linux - Freedom, Friends, Features, First
  - Innovation mayhem (i.e. glibc, systemd, selinux)
- Red Hat Enterprise Linux
  - Enterprise quality product
  - Strong security – Common Criteria, FIPS-140
  - Long term support
- DNSSEC fits in this model
  - Deploy in Fedora first
  - Carefully merge into RHEL later



Paul Wouters <pwouters@redhat.com>

The basis: Fedora and EPEL packages

- Multitude of DNSSEC packages
  - resolvers: bind, unbound, libval
  - authoritative: bind, nsd, pdns
  - signers: bind, opendnssec
  - tools: validns, dnssec-tools, dnssec-check, dnssec-system-tray, mozilla-extval, dnssec-nodes
  - dnssec-trigger
  - hash-slinger (formerly sshfp, now with tlsa support)
  - openswan with dnssec support
- All the tools are there to build signers, resolvers, validators

Paul Wouters <pwouters@redhat.com>

Fedora infrastructure

fedora HOSTED
START A PROJECT. WATCH IT GROW.

- First to enable DNSSEC (and DLV) per default when installing a resolving name server
- First to ship DNSSEC keys before a signed root using dnssec-conf (discovered “rollover-or-die” bug in bind)
- fedoraproject.org first signed Oct 3 2009 (DLV, no DS)
- Publishes TLSA records for fedoraproject.org

- Hotspot detection and login page at:
  http://fedoraproject.org/static/hotspot.txt
  http://hotspot-nocache.fedoraproject.org/
- Runs open DNS resolvers on TCP (port 80 and 443)

Paul Wouters <pwouters@redhat.com>

DNSSEC experience: #1 Captive Portals

- dnssec-trigger + unbound = okay (but not great)
  - Try cache, then full resolver, then TCP 80, then TLS
- Need better integration with Network-Manager
- Monitor and act on Web and DNS hijacking together
- dnssec-trigger needs to reconfigure unbound for more aggressive retries, shorter negative caching
- unbound needs support for querying DNSSEC chains
  - 1 query per HTTP/TLS connection does not work

- **Excellent co-operation with NLnetlabs**

Paul Wouters <pwouters@redhat.com>

DNSSEC experience: #2 VPN using Openswan

- Openswan reconfigures unbound
  - IPsec XAUTH parameters received contain domain name (“redhat.com”) and nameservers (“1.2.3.4”)
  - When the VPN is established it runs unbound-control to configure forwarder, flush cache for “redhat.com” and flush request list.
  - When VPN disconnects it runs unbound-control to remove forwarder, flush cache for “redhat.com” and request list
  - Works very well, except when VPN silently times out (happens when using OTK, i.e. SecureID)
- Openswan patch: use libunbound not gethostbyname()

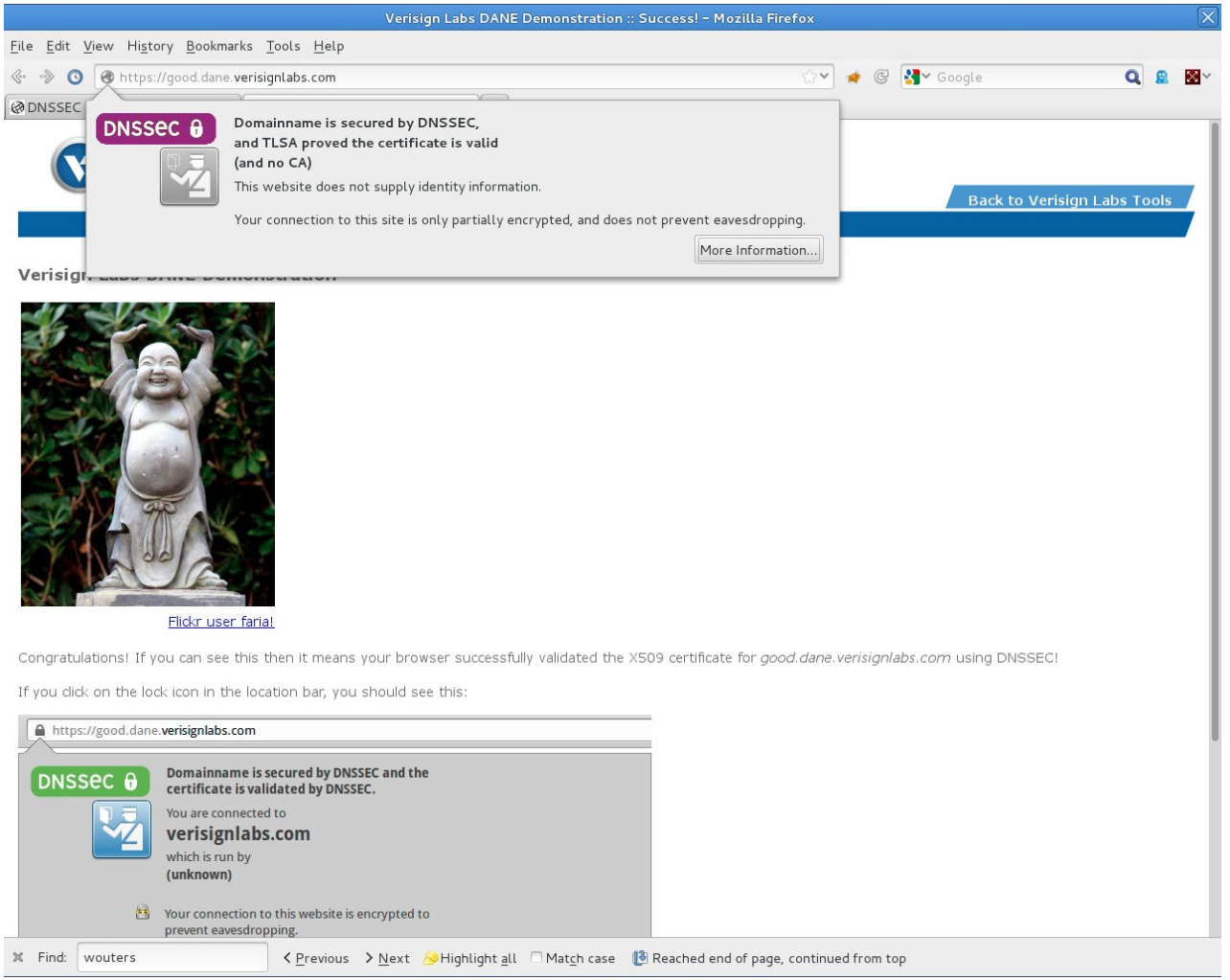
Paul Wouters <pwouters@redhat.com>

DNSSEC experience: #3 Split DNS

- Simple split DNS (eg VPN) works
- More complicated when external and internal zones are signed – “DNS lying” is required due to DNSSEC
  - Running your own resolver means using public view
  - internal.redhat.com does not exist in public view
- Patched unbound to support distributing trust anchors (i.e. via puppet)
  - /etc/unbound/keys.d/internal.redhat.com.key
  - /etc/unbound/conf.d/internal.redhat.com.conf
  - /etc/unbound/local.d/nasa-override.conf
- We need more experience with complicated DNS splits

Paul Wouters <pwouters@redhat.com>

TLSA Validator for Firefox



Paul Wouters <pwouters@redhat.com>

Generating TLSA and SSHFP records is easy

- yum install hash-slinger
- tlsa –create www.example.com
- sshfp -a (known_hosts)
- sshfp -a -d -d nohats.ca -n ns0.nohats.ca (axfr+scan)

Paul Wouters <pwouters@redhat.com>

DNSSEC: RHEL integration

- Wait on more experience and stability with Fedora
- As a server OS, captive portal not as important, but RHEL as desktop gaining traction and under increased security demands
- Only allowed crypto libraries: NSS, openssl, libgcrypt
  - libunbound can now use NSS instead of openssl
  - The unbound daemon still requires openssl
  - OpenDNSSEC uses botan which is not certified
- Running in FIPS mode still causing problems
  - MD5 not available (unbound, nsd,...)

DNSSEC: TODO list

- Support in Anaconda / NetworkManager to run validating resolver on every install (for Fedora 19?)
  - resolv.conf with only 127.0.0.1 makes everyone happy!
- Integration of dnssec-trigger and NetworkManager
- DNSSEC chain support for TCP queries (IETF work)
- Single storage of root and DLV keys
  - applications cannot yet be guaranteed a local resolver
  - Multiple formats, multiple locations
- Long term handling of shipping DNSSEC keys, especially the root key. Grab RHEL7 from a shelve in 2020 and turn it on, will DNS still work?

Paul Wouters <pwouters@redhat.com>

Questions?

Find the guy with the red hat after the panel discussion