Secure Boot. In Debian. In Buster. Really.

Steve McIntyre <93sam@debian.org>

21st July 2019

Agenda

- This is a BoF!
- What is UEFI Secure Boot?
- In the Linux world, and in Debian
- The awkward (and good!) bits
- Gobby doc – please take notes
  - gobby.debian.org
  - `Debconf19/bof/SecureBoot`

What is UEFI Secure Boot?

- Signatures on boot-time binaries
- Firmware includes public keys, checks signatures
- Designed to stop boot-time malware
- Most modern x86 machines include it
- Can be disabled if desired

In the Linux world

Shim – simple first-stage bootloader

- Collaborative project amongst distros
- Binaries ~~reviewed~~/signed by Microsoft
- Embeds further keys
- MOK
- Verifies and starts next stage (Grub)

In the Linux world (2)

- Further binaries signed with distro key
  - Grub
  - Linux
  - fwupd/fwupdate
- Restrictions on functionality
  - No unsigned kernels
  - No hibernation
  - etc.

Supported in Debian?

YES!

Working in Debian

- Support for 3 architectures
  - amd64, i386, arm64
- Packages using Recommends
- Should work invisibly:
  - d-i (CD/DVD/USB/netboot)
  - Live media
  - Installed systems
  - Cloud images...

Debian infrastructure

- -signed and -unsigned packages
- -signed-template pseudo-source packages
- Signing service
  - Locked down
  - Keys in HSM
- 2 buildd passes

The awkward bits

- It’s taken a very long time
  - Why?
  - Cross-team collaboration
    - Kernel, EFI, FTP, DSA, Buildd
  - Scaling of effort in Debian
  - Sprint in 2018

The awkward bits (2)

- Tooling is not very friendly
  - Security-related software
  - With maybe 50 users worldwide
- Issues
  - More firmware, more bugs
  - Non-free drivers

The good bits

- Easier installation
  - Less fighting with system setup
- Better support for secured systems
- User freedom
  - User-controlled keys
  - Options for Free Software end-to-end

Thanks to everyone!

- Team effort
- Lots of work

What else?

Discuss!