UEFI and Secure Boot in Debian

Steve McIntyre <93sam@debian.org>

17th November 2013

Current state

- EFI **boot** for ia64 since forever (elilo)
- Wheezy UEFI **boot** (grub-efi)
    - d-i should work on amd64 UEFI machines, CD / USB boot
    - I386 (U)EFI might work, but not supported
- It's grotty, but it mostly works
    - Some known bugs

What's left?

- UEFI PXE boot
- UEFI for other architectures
  - armhf, arm64, ...
- Bug fixes

UEFI stub or bootloader?

- UEFI → stub for direct kernel boot
  - Potentially faster
  - Not useful for generic use
- UEFI → Gummiboot → stub kernel
  - Maybe?
- UEFI → grub → kernel
  - Vastly more flexible
  - Right choice for Debian?

Secure Boot

- Debian does not support this (yet)
- Do we want to?
  - Do we get a choice?
- Some work to do

Shim

- Written by Matthew Garrett for Fedora
- Used (and extended) in other distros
- Signatures and checking
- Getting things signed
  - Archive infrastructure

SB Implications for x86

- MS logo requirements for Windows 8
- Must be able to disable signature checking
- Must be able to use your own key(s)

SB Implications for ARM

- MS logo requirements for Windows 8
- Must **NOT** be able to disable signature checking
- Able to use your own key(s) ?

SB work to be done

- Shim packaging etc.
- Archive support and process
- Grub (other bootloaders?)
- Installer
- ...?
- Who's doing it?