Linux Kernel Crypto API

Herbert Xu
Red Hat Inc.

Current State

- Async + sync cipher interface.
- Async + sync hash interface.
- AEAD interface.
- Compress-as-you-go interface.
- RNG interface.

Current State

- A handful of async PCI drivers.
- Support for on-chip acceleration.
- AEAD algorithms: CCM/GCM.
- Disk encryption algorithms.
- Mandatory self-test.

Generic Algorithms

- DMA offload similar to crypto offload.
- Reduce impact on generic code (e.g., TCP).
- New algorithms:
  - memcpy: Similar to ciphers.
  - xor: Binary operation.

User-space API

- Why:
  - Hardware management.
  - Certification.
- How:
  - Type-agnostic.
  - IOV-based interface.

Misc

- New algorithms:
  - Hashes.
  - Stream ciphers.
- User-space control interface.

Questions