Google

Encrypting Android Devices

Linux Security Summit 2015

Paul Lawrence and Mike Halcrow, Google

Agenda

- Why encrypt?
- State of Play
- State of Play - issues
- Platform Requirements
- EXT4 Encryption
- EXT4 and F2FS Encryption (and beyond)
- Performance
- Future Directions

Why Encrypt/Mobile Adversarial Model

- Left in bar/stolen device
- Evil maid
- Internal vs. SD Card Storage
- Confidentiality vs. Integrity

State of Play

- Full disk encryption of userdata partition
- dm_crypt, AES-128 and CBC with ESSIV
- Unlock screen at boot tied to primary user's account
- Unlock key linked to Trusted Execution Environment
- Some devices (Nexus 6,9) default encrypted, for most encryption optional

State of Play - Issues

- Unlock on boot, no functionality before that point
  - Accessibility
  - Incoming phone calls, messages
  - Alarm calls
- Only primary user can unlock
- Once unlocked, always unlocked
- Users/profiles have no separate keys

Platform Requirements

- Support diverse hardware from OEMs
- Provide strong encryption with short passwords
- Kernel diversity, age
- Flexibility - could not lock OEMs (or Google) to a specific filesystem (ext4)

Encryption Mode: ext4 encryption

- Initial implementation is as ‘drop-in’ replacement for dm_crypt
- Gives immediate benefits:
  - Secure user wipe
  - OTA updates easier
- Security
  - AES-256 in XTS mode
  - Encrypt file contents and file names
- Gives framework for future direction

Encryption Mode: ext4 encryption

- Non-user-specific folders encrypted with owner's key
- User folders encrypted with per user key
- All keys installed at boot time
- Run time policy checks
- Uses fstab flag /fileencryption
- Uses unencrypted folder to store (encrypted) key material, replacing the metadata partition

EXT4 and F2FS Encryption

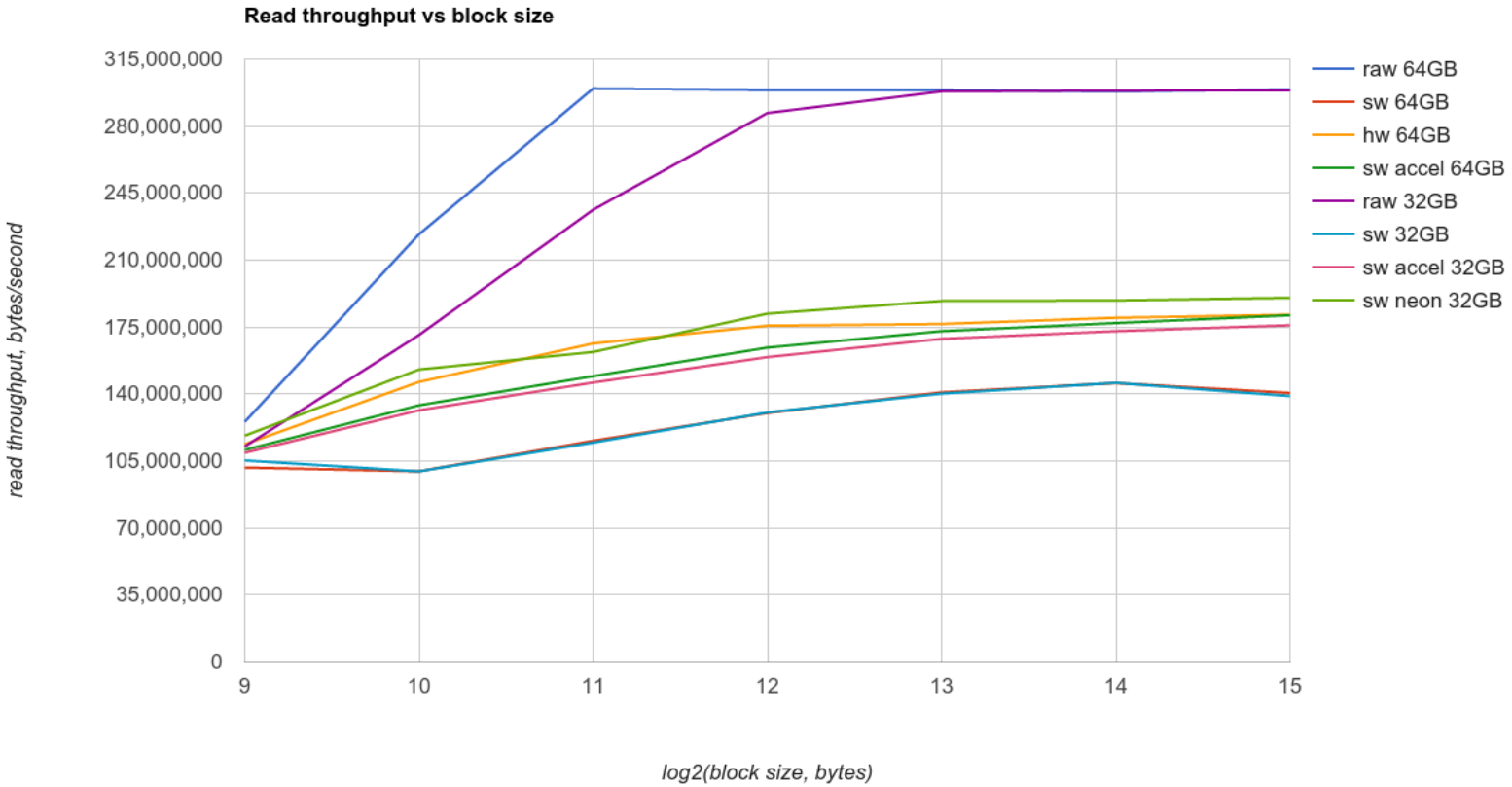
- EXT4 encryption upstream in kernel release 4.1
- F2FS based its per-file encryption on EXT4 encryption; in 4.2-rc
- Lots of copy-and-paste, suggesting a need for support for file-granular encryption in the VFS
  - Format for metadata and keys
  - Per-file random-access block encryption algorithms: key derivation, IVs, etc.
  - Mechanism for bounce pages on write path
  - Decryption in asynchronous read completion

Performance - Background

- Encryption has high impact on raw I/O numbers
- Encryption has little impact on day to day usage
  - e.g. Nexus 5 has 3% battery impact on streaming HD videos
- Occasionally we find an activity that reflects raw impact
  - e.g. starting one popular app requires 100MB of raw I/O and on a low powered ARM device adds five seconds to launch time due to 20MB/s decryption speed

Performance - Hardware

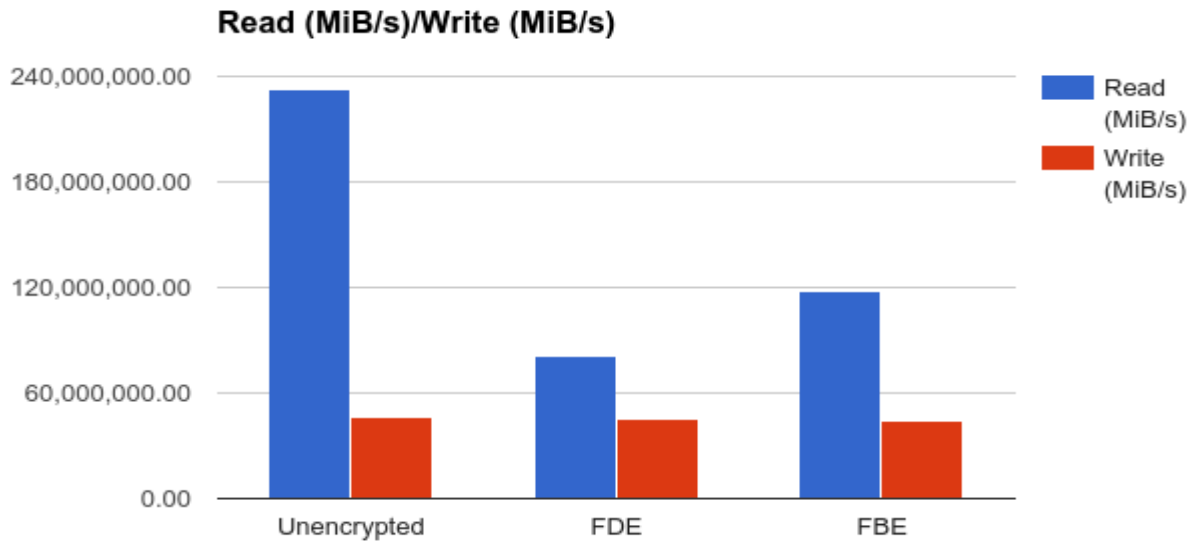
- For ARM devices we have
  - Software crypto
  - NEON accelerated software crypto
  - ARM v8 AES instructions (Nexus 9)
- Pure crypto hardware


Read throughput vs block size
315,000,000
280,000,000
245,000,000
210,000,000
175,000,000
140,000,000
105,000,000
70,000,000
35,000,000
0
9
10
11
12
13
14
15
read throughput, bytes/second
log2(block size, bytes)
raw 64GB
sw 64GB
hw 64GB
sw accel 64GB
raw 32GB
sw 32GB
sw accel 32GB
sw neon 32GB

Performance - ARMv8

raw	sw crypto
131,277,202	123,881,204
131,396,051	130,046,515
131,408,916	129,992,958
131,402,441	130,087,468
131,392,810	132,783,670
132,629,498	132,204,915
132,665,564	132,977,719

Throughput


Read (MiB/s)/Write (MiB/s)
240,000,000.00
180,000,000.00
120,000,000.00
60,000,000.00
0.00
Unencrypted
FDE
FBE
Read (MiB/s)
Write (MiB/s)

Latency

- On a test device, open for read goes from 13 microseconds to 67 microseconds
- Peak activity of 200 file opens per second
- Worst case then is 54 microseconds * 200 opens for 10.8 milliseconds per second performance hit - 1% even if we ignore multiple cores
- As with throughput, easy to imagine an app that shows a much higher impact than this

Future Directions

- Integrity
  - If you don’t have data integrity, you very well may not have data confidentiality either
  - 2011 Attack against XML encryption in Apache Axis2: 1 byte of plaintext for every 14 rounds of ciphertext manipulations
  - Necessary properties: IND-CCA2, IND-CPA
- File system Metadata
  - Directory structure, file sizes, etc.
- VFS support
- More user features

Questions