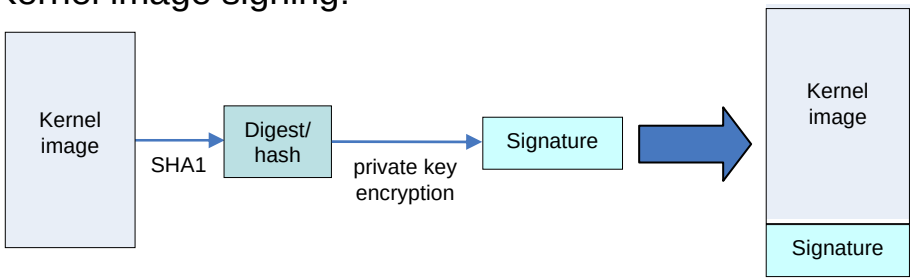
Secure Boot Loader

Stephen Johnson, Security Working Group

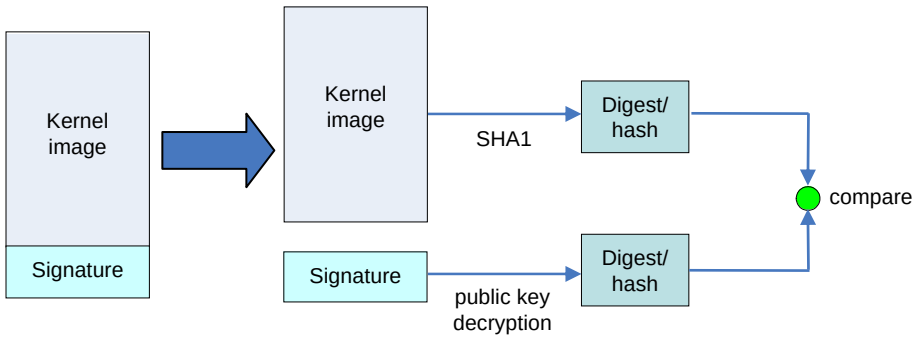
What is demonstrated

Secure booting using signed kernel images

Kernel image signing:



Kernel image verification:



Hardware Information

OMAP5912 OSK development system

How was the Linux improved

Uboot was extended to verify images using an RSA signature.

```
puts ("   Verifying Signature ... ");
if (verify_signature(hdr->ih_sign,
                     data,
                     len) == 0) {
          puts ("Invalid image signature¥n");
          SHOW_BOOT_PROGRESS(-3);
          return 1;
}
puts ("OK¥n");
```

During boot the meta-data is stripped from the image and the signature field is decrypted using the public key giving digest-1. Digest-2 is calculated directly from the image. These two digests are compared – equality means the image is undamaged.

Patch Availability

Will be released when completed.