Secure Boot Loader

Stephen Johnson, Security Working Group

What is demonstrated
Secure booting using signed kernel images

How was the Linux improved

Uboot was extended to verify images using an RSA signature.

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.