

STILL NOT CONVINCED

Too complex to apply to a locked down target with zero knowledge?

How to detect code exec?

- easy!

- fill entire unused flash space with NOPs
- monitor SPI address access

Image Headers

Original Signed Image

NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP

Unused Flash Area

NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP
NOP NOP NOP NOP NOP NOP NOP NOP

THIS WILL BE EASY

Nothing is easy.

- USON/WLCSP
- QSPI Decoder
- NGSCOPE?!
- Antenna wires

