**Bonus:**

Take Control of an ARM Chromebook

- The Samsung Arm Chromebook has “restricted” boot
  - (They call it “verified boot” or VB)
  - Google “root” key locked in flash with HPM
  - Have to disassemble hardware to unlock
  - Even then, no support for changing keys
- U-boot is locked in 4MB SPI flash, so we know how to read/write it, even if bricked (busprate)
- This talk explains how, and scripts/details are on sourceforge
- Note:
  - VB has been upstreamed into u-boot (cool!)
  - But is too large (700K) for most embedded use
Normal Verified Boot (VB) Flow

This is a “locked bootloader” aka “restricted boot”!

To take control, you have to replace “Root PK” with your own
Developer Mode

OS verification is OFF
Press SPACE to re-enable.
Non-Verified Boot Flow

SoC
- Boot ROM

SPI Flash
- Preboot
  - SPL
  - RO u-boot
  - Root key
    - Firmware key
    - Kernel subkey
  - RW u-boot

MMC Flash
- NV u-boot
  - Kernel key
  - Kernel
SPI Flash HPM:
!WP shorted to ground
SPI Flash Write protection

W25Q32DW status registers

SR1                      SR0
7  6  5  4  3  2  1  0  7  6  5  4  3  2  1  0
^srp1  ^srp0  ^...BP...^

0  0  1  1  1  0  0x0038  OFF
0  1  1  1  1  0  0x00B8  HPM
1  0  1  1  1  0  0x0138  POWER

flashrom options:
   --wp-status
   --wp-enable[= hardware | power_cycle]
   --wp-disable

Flashrom -p internal:bus=spi --wp-enable=power_cycle --wp-status
WP: status: 0x0138
WP: status.srp0: 0
WP: status.srp1: 1
WP: write protect is enabled.
WP: write protect range: start=0x00000000, len=0x00200000
Taking Control

1. Disassemble Chromebook and remove !WP washer
2. Enter “Developer” mode (esc-refresh-power)
3. Copy scripts to somewhere executable (/usr/local/takeown)
   - (ctl-alt--->), login as chronos, sudo -i
   - ./makekeys.sh (makes all new key pairs)
   - ./takeown_firmware.sh (signs RW u-boards and keys)
   - ./takeown_kernel.sh (signs kernels and keys)
   - dev_debug_vboot (verifies all keys/signatures)
4. Modify RO u-boot to set power_cycle protection, if not developer (experts only)
5. Save keys to usb, reboot, and follow prompts for normal mode
DaveOS

- A really hard way to demonstrate SPI control

OS verification is OFF
Press SPACE to re-enable.
Chrome OS is missing or damaged. Please insert a recovery USB stick or SD card. (note: the blue USB port will NOT work for recovery)
Buspirate Attached to SPI Flash
Close up of SPI Flash

!WP washer removed

Battery disconnected
<table>
<thead>
<tr>
<th><strong>SPI Flash</strong></th>
<th><strong>Bus Pirate</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CS (pin 1)</td>
<td>---- CS</td>
</tr>
<tr>
<td>CLK (pin 6)</td>
<td>---- CLK</td>
</tr>
<tr>
<td>SI (pin 5)</td>
<td>---- MOSI</td>
</tr>
<tr>
<td>SO (pin 2)</td>
<td>---- MISO</td>
</tr>
<tr>
<td>V+ (pin 8)</td>
<td>---- 3.3v</td>
</tr>
<tr>
<td>GND (pin 4)</td>
<td>---- GND</td>
</tr>
<tr>
<td>!WP (pin 3)</td>
<td></td>
</tr>
<tr>
<td>!hold (pin 7)</td>
<td></td>
</tr>
</tbody>
</table>
All Code available

- Chrome takeown

- mr-3020 secure boot: