PS3 Console Hacking

2/8/17

* PS3 architecture
  + SPU-use for security
    - read,write to see what is being done
  + LV1/Hyperviser
    - Available spu
  + LV2/GameOS
    - Available spu
  + Problem state/games
  + Lv0
    - Launch powerpc
  + Has on-de bootROM, public-key crypto, chain of trust, per-console keys, signed executables, security coprocessor, encrypted storage, hypervisor, user kernel mode.
* Other OS
  + Virtual memory
    - Page table saves the locations of the data that belongs to the virtual memory from the RAM
* Device 4
  + Configuration #1: interface #1
  + Configuration #3 gains LV2 code access
* Hypervisor allows unsigned code on PS3
  + Allowed on xbox360
  + You can run code on patched lv2 from hdd
* AsbestOS
  + Replace lv2/gameOS in memory
  + others mode and gameOS mode are virtual identical
    - except gameOS can do more
  + (S)ELF-extensible library format: (secure)elf
* The Oracle
  + Decrypting all code possible from gameOS
  + Possible for anyone to encrypt in OS
* SPE
  + Controlled by PowerPC
  + Checked verification list came from sony
* Sign w private key and check to public key