Xbox 360 Hacking

* Exploiting the HV
  + All user code interacts with most hardware directly
  + Only cpu internal registers and the mmu are handled
* Twice the trouble
  + Cmplwi will ignore bits set in the upper 32bit
  + Rldicr andlwz will not
  + Allows attacker to set some upper bits in the address (bits 34 to 63 can be set arbitrarily)
* Get Penguins on Board!
  + Minor glue code for smp, interrupt handling timer, pci enumeration, sata
  + Drivers for Ethernet, framebuffer, 3d were written