Hardware and Media Security

1/25/2017

X-Box Security

1. Avoid Bios Hacks
   1. Don’t store bios on separate flash rom
      1. Put on chip
      2. Either chip with flash-rom are built in or no updates
   2. Have your bios signed cryptographically
2. What goes wrong
   1. Andrew “bunnie” huang sniffs encryption key
3. What else goes wrong
   1. 2bl uses jam table to help in initialization
4. Jam-table
   1. Write in location 0x0000.0000
   2. 0xffff.ffff rolls over to 0x0000.0000
5. Microsoft Reaction
   1. New Security Scheme completely replace Southbridge chip in new X-Boxes
   2. NVidia
6. Software hacks
   1. Buffer overflow in saved memory
   2. Memory card attached to controller
      1. Controller uses usb
      2. Plug some usb drives in and have them work as memory card (or vice versa)
7. Game cheating
   1. Microsoft is selling x-box live online services
   2. Cheating on-line games not good with microsft.