HARDWARE SECURITY

WHAT IT IS, HOW IT WORKS, AND WHAT YOU CAN DO ABOUT IT
OUR TITLE: RESEARCH ASSISTANT

• What we did:
  • Read lots of research papers
  • Design VHDL code to specifications
  • Wrote up experiments including the hardware we built
WHAT WE LEARNED

• Lots of Research Papers

• Fewer practical applications
  • Most prominent example: Defeating Xbox Region Locking

• Hardware Security == Fight Club

• Most of the effective strategies rely on physical security of the hardware involved
  • Hits to hardware performance and/or device cost have left security out
  • This is changing with computer performance increases
HARDWARE TROJANS

• The anti-art of breaking stuff by putting in unwanted functions

• Famous examples:
  • Backdoor
  • Time bomb
  • Malicious errors

• Inserted by:
  • Fabrication Facility
  • Unethical Engineers
  • Used for testing and not removed from production hardware
BUS SNOOPING

• The bus is the connection set between your CPU and memory
• Data on this is almost always not encrypted
• EVERYTHING a computer does crosses this connection
• “Snooping” is watching what happens over this connection
  • Can be with an oscilloscope or with specialized software depending on the system
• Requires physical access to hardware
PHYSICAL UNCLONABLE FUNCTION

- Method of authenticating hardware
- Works by challenging the PUF and getting a response
- Xbox used this for region lock
- Defeated by interface between PUF and main system