Bootjack: BIOS Implant Detection

Program Manager: Mr. Richard Guidorizzi, DARPA, I2O

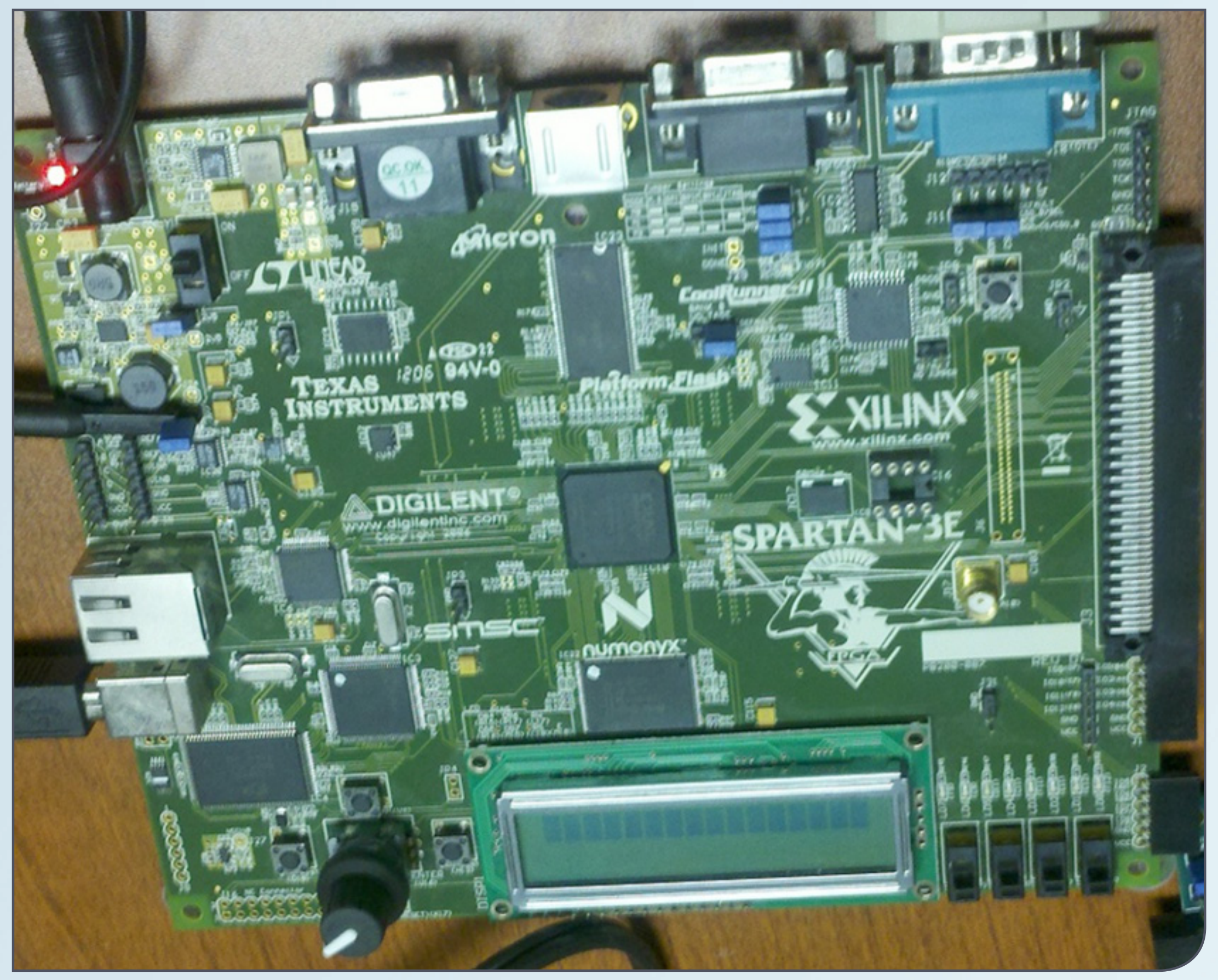
Selective Intellect, LLC
Technology Readiness Level 5

Project Summary

- Bootjack provides a configurable hardware solution for detecting compromised BIOS components on personal computers.

Project Description

- Most computer motherboards are equipped with a BIOS for booting the machine into an operating system (OS) such as Windows or Linux. BIOS-based rootkits (bootkits) can be planted by malicious attackers using various methods. A compromised BIOS is invisible to modern antivirus tools, and may remain persistent across hard drive formatting and operating system installs.
- This project built Bootjack to detect whether the BIOS has been compromised.
  - When plugged into a USB port, the Bootjack ARM-based board identifies itself to the BIOS as a bootable USB disk drive.



Bootjack created a hardware device that detects BIOS rootkits in seconds.

- When the machine is rebooted, the BIOS tries to load the OS from the faux Bootjack USB disk drive, which in turn scans the BIOS.
- When the verification is complete, the ARM-based board informs the user via the screen or through light-emitting diodes (LEDs) on the board if the system BIOS has been compromised.