SAND2010-0086C

LPC/SPI Analysis Tool

Tiffany A. S. Pierce and Michael Berg, Christopher Hoff, Brent Kucera

Sandia National Laboratories*
Albuquerque NM, USA, 87185-0620
tasuski@sandia.gov

Abstract: *A team at Sandia National Laboratories has created a set of hardware tools to analyze Low Pin Count (LPC) and Serial Peripheral Interface (SPI) bus traffic in desktop and laptop machines. The equipment includes generic prototyping and analysis boards combined with custom parts to capture LPC/SPI traffic. The LPC/SPI analysis equipment attaches directly to the headers on a motherboard for passive capture. Also under development are custom software tools that support filtering, parsing, and searching of the bus traffic. In some cases, the software may be used to send commands to either LPC-based or SPI -based components on special host boards. The functionality that this prototype system provides may help support vulnerability analysis, debugging hardware components and device drivers during development, and exercising functionality for acceptance testing.*

Keywords: Low Pin Count; Serial Peripheral Interface; hardware debugging; traffic capture; protocol analysis.

Introduction

A Sandia National Laboratories research team has developed tools to analyze Low Pin Count (LPC) and Serial Peripheral Interface (SPI) bus traffic in modern computers. The LPC/SPI analysis tool is a combined hardware and software system that contains some customized circuit boards. To analyze LPC or SPI traffic, the appropriate circuit boards are plugged into a bus header on the motherboard of the machine under test. The hardware sends captured traffic to a Windows-based software client, usually located on a separate analysis computer. In cases where analysis of a device on a motherboard is impractical, it can be isolated on a special host board and the software client can generate data and commands to operate it.

The LPC/SPI analysis system is currently in a prototype stage and has not been used for a wide variety of applications. However, the data capture and filtering capabilities of the LPC/SPI analysis tools should enable vulnerability analysis, acceptance testing, and hardware debugging activities for any computer components that communicate using the LPC or SPI bus. This includes SPI devices like flash and EEPROM memory, Ethernet and USB communications, real-time clocks, and temperature sensors. LPC bus devices that can be analyzed include serial and parallel port I/O devices like the keyboard and mouse, floppy disk controller, boot ROM for a legacy BIOS, and Trusted Platform Modules (TPMs). To aid in the analysis of these components, some tools for parsing and issuing commands at a higher level have been developed and integrated into the analysis software.

The equipment used to analyze a device varies slightly based on application. Refer to Figure 1 for the two most common configurations. More detailed description of the hardware and software components of the system can be found in subsequent sections, but in general conducting vulnerability analysis or testing with the LPC/SPI analysis tool requires the following components:

- Altera FPGA prototyping board with custom software and firmware
- Custom circuit board attachments for either passive or active analysis
- Device under test (DUT) on the LPC/SPI bus of a computer motherboard
- Analysis software client on a separate analysis machine

System Components

FPGA Development Board: The generic Altera FPGA development board hosts custom firmware developed by the team to capture, buffer, and filter the LPC or SPI data. It also has an Ethernet network controller that handles communications needed to send data to the software client. The firmware is designed so that it can be easily modified to support customizable filtering or triggering to support precise analysis. These kinds of features can be useful if the buffering and communication delay inhibits debugging activities for a specific device or intent.

Custom Analyzer Boards: The analyzer boards are designed to connect the FPGA board to LPC or SPI bus headers on the motherboard. Depending on the analysis goals, these custom boards might also have pin headers so that a separate logic analyzer may be attached to monitor clock or data lines on the bus. These analyzer boards are necessary for passive analysis to support plugging in to a variety of header configurations that may be available on modern motherboards.

* Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

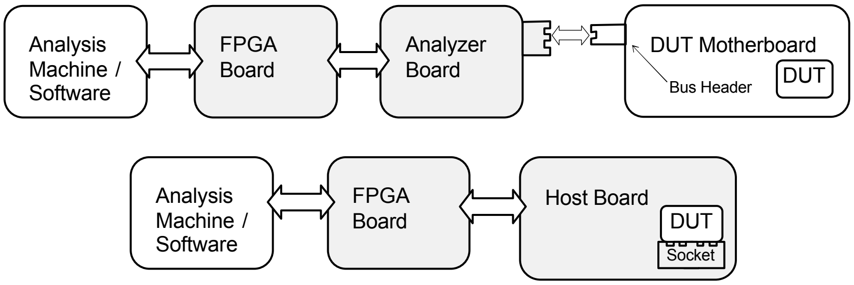

Figure 1. Equipment needed for two different LPC/SPI analysis configurations. The system can be used for either passive analysis of an in-situ device (top) or analysis and exercise of an isolated part on a custom host board.

Custom Host Boards: The FPGA development board also supports the attachment of custom host boards: circuit boards that can host a socketed LPC or SPI device if a working motherboard is not available. The host boards must supply power and clock lines to the device and support communication. Data or commands sent to the device generally originate in the software client and are then sent through the FPGA board to the device under test. The FPGA board then accepts and routes device responses back to the software client.

LPC/SPI Analysis Software Client: The Windows-based software client operates on a separate machine from the device under test and supports additional filtering, parsing, searching, and display of LPC/SPI bus traffic. Since many different components may be communicating via the LPC and SPI buses and there may be significant amounts of time between data of interest to an analyst or debugger, this capability is quite useful. For example, the system can search data packets by address, read and write direction, and data contents. It can also filter and display only LPC or SPI events associated with protocol errors.

The client can be extended to parse commands and data for particular devices and display the information in a more human-readable and useful format. For proof-of-concept purposes, extensions have been developed to identify, parse, and build commands for some devices on the LPC bus.

LPC/SPI Passive Analysis

Motivation: Some commercial LPC and SPI protocol analyzers exist, and they are usually based on standard logic analyzers with some additional software. These analyzers may be difficult to use when targeting a specific device on a machine with many other components communicating on the same bus. The quality and usability of such systems vary by vendor and purpose.

The goal of this project is a flexible software client that can be used to analyze and interpret both LPC and SPI bus traffic with easily customizable searching and filtering abilities. Collecting and saving the data on a separate analysis machine helps avoid problems related to resolution of captured data traces and provides plenty of memory to save and store data. The format of the data can be easily modified or converted if needed to be compatible with more sophisticated or powerful analysis tools. As an example of the challenges involved in analyzing bus traffic without automated tools, Figure 2 depicts traffic across the LPC bus as shown by a logic analyzer. The logic analyzer is able to interpret the values of the data on the bus, but it is difficult to parse and view large amounts of traffic at one time.

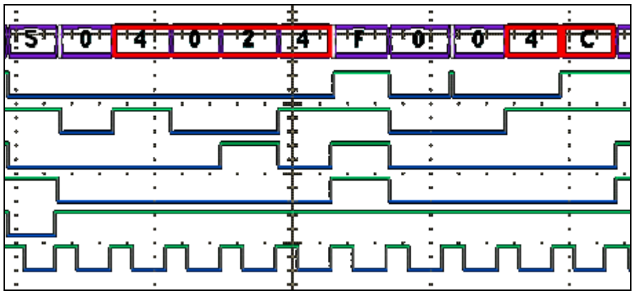

Figure 2. LPC bus traffic viewed with a logic analyzer. The individual lines are interpreted together as data values in the top line of the display.

Generally, passive analysis is accomplished by attaching the FPGA development board to an analysis machine using an Ethernet cable, and attaching the analyzer board to the FPGA development board. The analyzer board then plugs in to a bus header on the motherboard containing the DUT. Once the equipment is hooked together as shown in Figure 1, the bus traffic can be captured by allowing the machine containing the DUT to operate normally. For situations when a specific scenario is under test a user can usually trigger the functionality from the machine itself, either via custom drivers or by using an interface provided by the system.

LPC/SPI Active Analysis

Motivation: The complexity of modern computer systems may inhibit in-situ analysis of a component on a noisy motherboard. It is also possible that the functionality under test is not exercised in normal operating conditions or that the hardware drivers are incomplete. This is often the case with devices that are still under development or when a team is attempting to use third-party driver software. In such situations, it is valuable to bypass software drivers and unknown interactions altogether by isolating the device on a custom host board and sending LPC/SPI traffic directly from the software client.

This ability to exercise a loose device is helpful in debugging custom software/hardware solutions because it can help identify if an error is originating in the hardware device or in the software drivers. Also, some aspects of acceptance testing may require low-level interaction with the device, for example to vary the data speeds and conditions under which the device is required to operate. For acceptance testing, an analyst can generate test cases, data, commands, and conditions that are supported according to documented specifications, and then verify expected results.

Additionally, using the host board configuration can protect the other components in a system. If a device does not fail safely under some test condition on an isolated host board, there is no danger of damaging the rest of the system.

To conduct active analysis on an LPC or SPI device, the analysis machine is connected to the FPGA development board via an Ethernet cable. The FPGA board is connected to a custom host board with a standard ribbon cable. The design of the host board may vary based on the DUT; some may have more or fewer pins and need special sockets. The DUT is plugged in to a header or socket on the host board, and then the system is powered up and controlled from the software client. An example of this kind of configuration for active analysis is depicted in the lower part of Figure 1.

Potential Applications

This LPC/SPI analysis tool will be useful for a wide variety of applications. Its main uses involve profiling a system to characterize the behavior, debugging complex errors during development, acceptance testing (comparing required device specifications to actual device performance), and vulnerability analysis (an in-depth review of the system to ensure that security measures are both in place and correctly implemented). The system can analyze the communication traffic of any components that use either the LPC or the SPI bus. Thus, it is potentially useful for analysis of components such as memory controllers, legacy BIOS chips, temperature and other sensors, serial and parallel I/O devices, and TPMs.

Hardware and Software Debugging and Testing: As previously mentioned, LPC/SPI analysis tool can be used to debug hardware that is in development and can be used to troubleshoot tricky problems by isolating bugs or tracing the cause of unexpected behavior. Generally, this could be the result of software-level driver problems, hardware-level bugs, or both. By capturing the hardware-level bus traffic, it may be easier to identify the causes of such errors. The software client can make it easy to identify protocol errors by filtering out the bus traffic that conforms to the protocols.

Also, if a project involves poorly documented or third-party device drivers this system can be used to verify that they operate as expected and to observe how variations in software parameters affect the hardware activity. These debugging and analysis steps can ensure that complex bugs are identified and caught early in the development cycle.

Acceptance Testing: Acceptance testing generally involves building and running many test cases according to published specifications or requirements. The LPC/SPI analysis tool can be used to assess whether a system operates in the way it was intended by comparing actual responses to expected responses. This is one way to determine if a component can be used as advertised. For example, if a device is advertised to be able to handle situations in which it is exercised very frequently, such high-load situations can be tested using the custom host board where conditions can be carefully controlled and there is no danger to other system components.

System Profiling: To characterize the behavior of a system or better understand the way it operates, the LPC/SPI analysis tool can help build detailed descriptions of memory usage during boot, shut-down, or normal operation. Similarly, it can be used to profile the use of or interactions between any LPC or SPI components. In this way an analyst can identify when and how the hardware components are handled by the BIOS and the operating system. Such information can be useful when checking for wear and usage problems that might lead to burnout early in the development process.

The analyzer board for passive analysis of the LPC and SPI buses allows the user to observe the bus traffic of the machine in normal operating circumstances from boot up to shut down. Another aspect of system profiling involves modifying the behavior or settings of the machine and observing how the bus traffic changes in subsequent captures.

Virtualization of Resources: One exciting application for this system involves analysis of hardware virtualization technology. Hypervisors and host operating systems may attempt to virtualize hardware resources so that each client may behave as if it has full use of the machine’s resources. The hypervisor controls the balancing and allocation of the physical resources in a way that is transparent to the guest users. The LPC/SPI analysis tools may be used to capture what is actually happening at a hardware level and compare it to what a guest operating system expects. Using these techniques, analysts can assess how effective the hardware virtualization is and whether it can be optimized for normal operating conditions. Resource optimization and conservation is important when providing an effective experience for the users.

If a virtualized resource is security-related (e.g. the TPM), the LPC/SPI analysis tools can help verify that the privacy and security of the guest systems is maintained by the hypervisor without compromising the performance of the system or of the TPM device. Research and analysis of the hardware-level effects of virtualization can help improve the quality of future virtualization technology.

Conclusion

The LPC/SPI analysis tool is a prototype-stage hardware and software system for sending, capturing, and analyzing LPC and SPI bus traffic. This technology is potentially useful in several areas including vulnerability assessment, acceptance testing, hardware and software debugging, and system profiling. Potential uses for this prototype tool include analysis of flash and EEPROM memory, Ethernet and USB communications, real-time clocks, temperature sensors, serial and parallel port I/O, boot ROM for a legacy BIOS, and Trusted Platform Modules (TPMs).

To support analysis and debugging activities the LPC/SPI analysis tool is capable of capturing, filtering, parsing, and searching data that occurs while the system is operating normally. Using a special host board, it also supports exercising a device while isolated from the rest of the system by controlling the host system from a software client.