SAND2014-16016D

FWTK:

Firmware Toolkit - Firmware Extraction

iSAFE
Interns for Security, Arms control and Force protection Engineering

Manager:
Shawn Taylor
6612/6613

Patricia Hurd
University of Tulsa
M.S. in CS, Dec 2014

Oliver Kubik
University of Maryland
B.S. in CS, May 2014

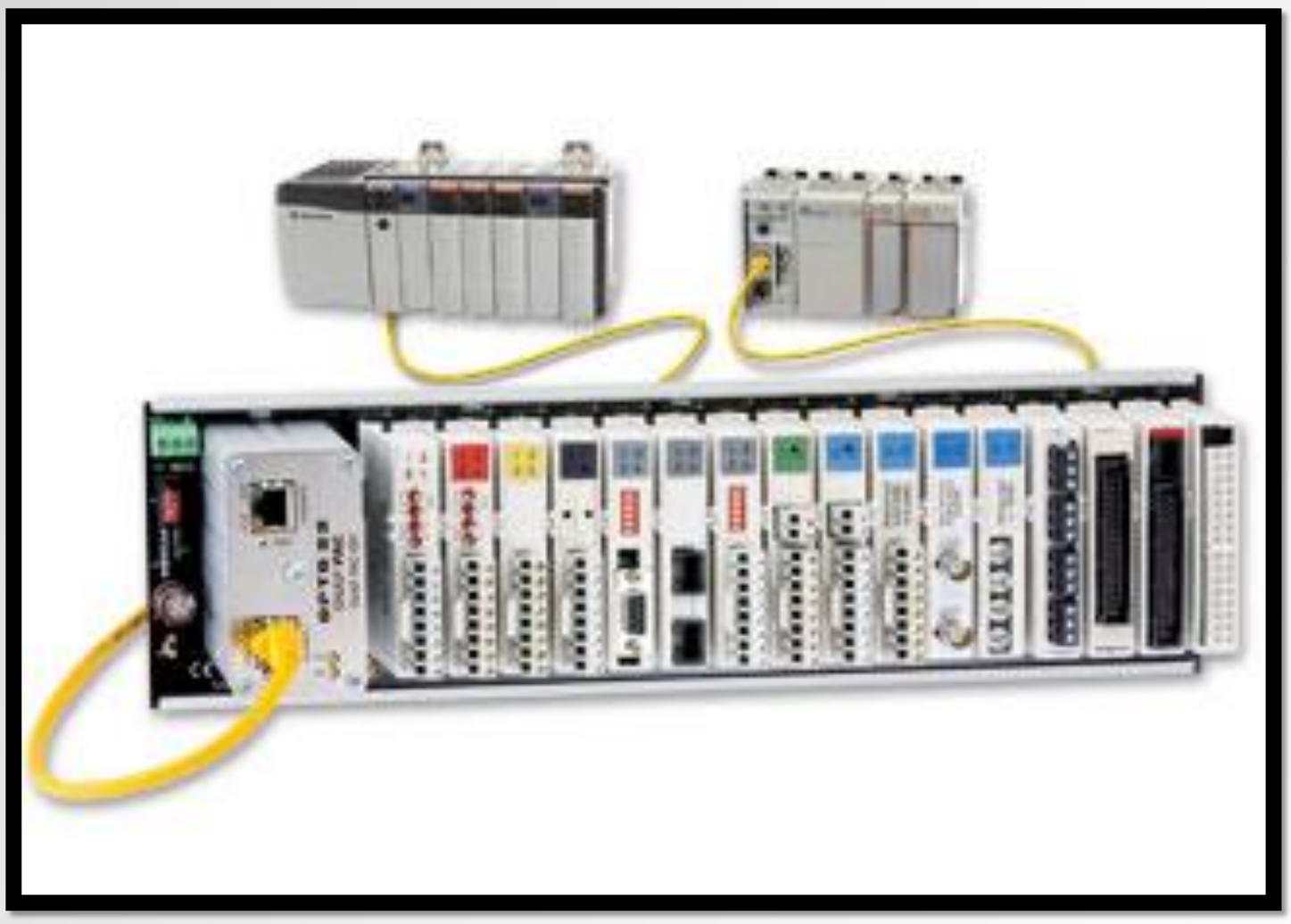
Kenny Lu
UCLA
M.S. In EE, March 2015

Co Authored with CCD Interns:
Jeremy Gin & Rachael Flores-Meath

Project Mentors:
John Mulder &
Susan Wade, 5628

When owners of a SCADA system suspect that it has been compromised, the integrity of the programmable logic controller's (PLC) firmware is one of the first things they might want to check. While it is typically straightfoward to obtain an original copy of the firmware from the vendor, obtaining a copy of the firmware on the device can pose some difficulty. Each vendor/device has a different mechanism for updating firmware, which means the mechanisms for retrieving the firmware are also different. While the firmware upload process is generally documented, the download process is not. Our goal is to analyze various systems and document the firmware download process.

The first step is to set up the software for the PLC and learn how to update the device firmware. Once the process for firmware update is understood, we can eavesdrop on the traffic being passed between the PLC and the computer by running Wireshark during a firmware update. Sometimes the update process uses standard application-level protocols like FTP, but often the protocols are vendor specific and require time-intensive manual packet analysis to determine the format.



Once the packet format is understood, Scapy can be used to write a custom parser for the captured traffic and to write a firmware update script. These update scripts not only check our understanding of the process, they also allow us to update the firmware without the (sometimes lengthy) software setup process for each vendor.

After understanding the firmware upload process, we can start to look for how to reverse the process for download.

Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2014-XXXXP

U.S. DEPARTMENT OF ENERGY

FWTK:

Firmware Toolkit - Firmware Extraction

Patricia Hurd
University of Tulsa
M.S. in CS, Dec 2014

Oliver Kubik
University of Maryland
B.S. in CS, May 2014

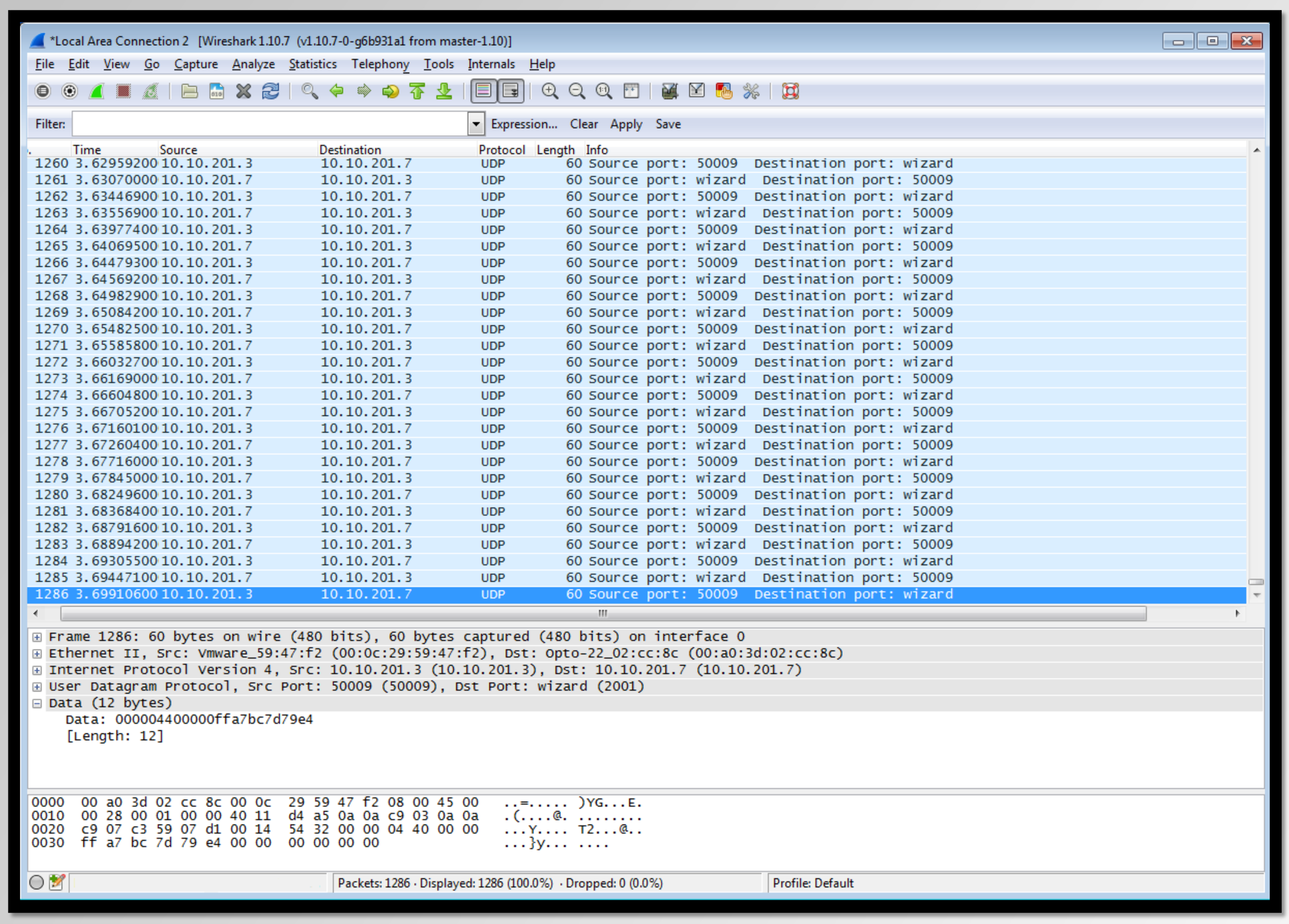
Kenny Lu
UCLA
M.S. In EE, March 2015

Co Authored with CCD Interns:
Jeremy Gin & Rachael Flores-Meath

Project Mentors:
John Mulder &
Susan Wade, 5628

Manager:
Shawn Taylor
6612/6613

Interns for Security, Arms control and Force protection Engineering



Results:

Opto22: We set up the software and monitored the firmware update; the upload uses passive FTP, but the process cannot just be reversed for firmware download since there is an intermediate step where the controller copies the firmware to flash, then deletes it. We tried reading the memory using the protocol provided by the vendor, but only the sections of the memory devoted to programming can be read. The next step will be looking at JTAG to dump memory.

Scadapack 32/350: Set up vendor software for PLC programming and firmware update. Listened to traffic, which uses Modbus/TCP. Vendor specific Modbus/TCP functions are used to read and write. Currently analyzing packets and attempting to send crafted packets to generate response.

Direct Logic 205: Monitored the traffic during a firmware update. The update uses a non-standard protocol; we created a python script with functions to help analyze the packet types and frequencies. We've identified certain packet types as well as some critical packets and the meaning behind certain bits, but additional work needs to be done before we can download the firmware.

Sandia National Laboratories

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2014-XXXXP

U.S. DEPARTMENT OF ENERGY