

Kennesaw State University
DigitalCommons@Kennesaw State University


KSU Proceedings on Cybersecurity Education,
Research and Practice

2016 KSU Conference on Cybersecurity Education,
Research and Practice

Towards an In-depth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets

Guillermo A. Francia III
Jacksonville State University, gfrancia@jsu.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/ccerp>

 Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Francia, Guillermo A. III, "Towards an In-depth Understanding of Deep Packet Inspection Using a Suite of Industrial Control Systems Protocol Packets" (2016). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 1.
<https://digitalcommons.kennesaw.edu/ccerp/2016/Practice/1>

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in KSU Proceedings on Cybersecurity Education, Research and Practice by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Abstract

Industrial control systems (ICS) are increasingly at risk and vulnerable to internal and external threats. These systems are integral part of our nation's critical infrastructures. Consequently, a successful cyberattack on one of these could present disastrous consequences to human life and property as well. It is imperative that cybersecurity professionals gain a good understanding of these systems particularly in the area of communication protocols. Traditional Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are made to encapsulate some of these ICS protocols which may enable malicious payload to get through the network firewall and thus, gain entry into the network. This paper describes technical details on various ICS protocols and a suite of ICS protocol packets for the purpose of providing digital forensic materials for laboratory exercises toward a better understanding of the inner workings of ICS communications. Further, these artifacts can be useful in devising deep packet inspection (DPI) strategies that can be implemented in network firewalls, in expanding challenge materials for cyber competitions, and in attribution, vulnerability assessment, and penetration testing research in ICS security.

Disciplines

Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Industrial Control Systems (ICS) are increasingly at risk and vulnerable to internal and external threats. These systems are integral part of our nation's critical infrastructures. Consequently, a successful cyberattack on one of these could present disastrous consequences to human life and property as well. It is imperative that cybersecurity professionals gain a good understanding of these systems particularly in the area of communication protocols. Traditional Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are made to encapsulate some of these ICS protocols which may enable malicious payload to get through the network firewall and thus, gain entry into the network. This paper describes technical details on various ICS protocols and a suite of ICS protocol packets for the purpose of providing digital forensic materials for laboratory exercises toward a better understanding of the inner workings of ICS communications. Further, these artifacts can be useful in devising deep packet inspection (DPI) strategies that can be implemented in network firewalls, in expanding challenge materials for cyber competitions, and in attribution, vulnerability assessment, and penetration testing research in ICS security. We also present software tools that are available for free download on the Internet that could be used to generate simulated ICS and Supervisory Control and Data Acquisition (SCADA) communication packets for research and pedagogical purposes. Finally, we conclude the paper by presenting possible research avenues that can be pursued as extensions to this seminal work on ICS security. Prominent among these possible extensions is the expansion of the ICS packet suite to include those protocols in the wireless domain such as Wi-Fi (802.11), Bluetooth, Zigbee, and other protocols that utilizes proprietary Radio Frequency.

The ICS protocol packet suite includes a representative sample of captured network packets on commonly used protocols such Distributed Network Protocol 3 (DNP3), Modbus Transmission Control Protocol (Modbus/TCP), International Electromechanical Commission (IEC) 60870.5, EtherNet/Industrial Protocol (EtherNet/IP), Common Industrial Protocol (CIP), and Ethernet for Control Automation Technology (EtherCat). For each of these protocols, a discussion on the frame structure is provided to help the reader gain a better understanding on how to interpret and analyze the captured file. For some of these captured packets, we demonstrate how to use Wireshark, a network packet analysis tool, to perform a deep packet inspection and analysis of the payload. We hope that this small contribution would stimulate the development of intelligent DPI systems dedicated to the protection of industrial controls.