ATTACK AND DEFEND TOOLS FOR REMOTELY ACCESSIBLE CONTROL AND PROTECTION EQUIPMENT IN ELECTRIC POWER SYSTEMS[1]

Paul W. Oman, Allen D. Risley, Jeff Roberts, and Edmund O. Schweitzer, III
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

The industry trend to increase the level of power system automation and remote accessibility, coupled with a dramatic increase in the number and sophistication of Internet and telephone based cyber attacks, is exposing the electric power industry to a growing risk of electronic intrusion. Furthermore, our electric power infrastructure is a potentially high-value target for individuals, organizations, and nations with anti-U.S. sentiments or political agendas. As a result, there is a very real and rapidly increasing probability that malicious individuals will attempt to gain remote access to your power control equipment in order to destabilize the power grid and/or destroy parts of your power system. Similar attacks have been launched against telecommunications companies and E-commerce sites for several years now. Fortunately, we can learn from their experiences. Many defensive techniques and practices have been used to reduce the chances of cyber attack and electronic intrusion, including password protection, audit logging, multi-tiered access levels, alarm conditions, remote authentication, redundant controllers, time-out communication parameters, virus protection, firewalls, encryption, and intrusion detection systems. However, to understand these defensive practices you first need to understand the offensive techniques that may be used to carry out a cyber attack or intrusion. In this paper, we describe the offensive techniques and capabilities of individuals (malicious and otherwise) so that you can counteract their actions with equally effective defensive measures. For each offensive procedure, we provide defensive tools and techniques that you can apply to your power system automation solutions. We note, however, that no system is ever 100 percent secure – only continued vigilance can ensure reliable operation of our electric power systems.

INTRODUCTION

The North American electric power grid is vulnerable to electronic intrusions (a.k.a. cyber-attacks) launched from anywhere in the world, according to studies by the White House, FBI, IEEE, North American Electric Reliability Council (NERC), and National Security Telecommunications Advisory Committee (NSTAC) [1, 2, 3, 4]. At the heart of this vulnerability is the capability for remote access to control and protection equipment used by generation facilities and Transmission and Distribution (T&D) utilities. Remote access to protective equipment historically has been limited to proprietary systems and dedicated network connections. Now, however, there is an increased use of public telephone services, protocols, and network facilities, concurrent with a growing, more sophisticated, worldwide population of computer users and computer hackers. These persons, regardless of location or nationality, represent a growing threat to the safety and reliability of electric power systems, and there is increasing evidence suggesting that United States infrastructures have been targeted by organized

[1] Portions of this work were funded by the U.S. Department of Commerce National Institute of Standards and Technology Critical Infrastructure Protection Grant #60NANB1D0116