News Release

The National Institute of Standards and Technology (NIST) adopts Vir2us' patented VMunity specifications in recommending cybersecurity for project 'Smart Grid' and the U.S. Government.

NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – July 2010 / Segmentation

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY/CYBERSECURITY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This National Institute of Standards and Technology Interagency Report (NISTIR) discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7628, vol. 3

(Excerpt from 9.6.9)

System Segmentation and the first principles of cyber security are isolation and defense-in-depth. The objective of this research is to develop methods to protect network end-points through Intense System Segmentation. The research should seek to create a platform that implements the characteristics of time-tested and recognized security principles. These principles include isolation, a minimal trusted computing base, high usability and user transparency, a limited privilege capability that provides for user, process, and application class of service definitions, and a default-deny rules engine enforcing such privileges. The requirement for continuous availability of Utility Grid operations necessitates a high degree of reliability within and across domains. Many domain end- points, such as legacy sub-station equipment, rely on outdated operating systems with little or no encryption capabilities, posing numerous challenges to the overall security of the Smart Grid. By enclosing an Intense System Segmentation framework around the existing computer architecture of these localized end-points, the legacy infrastructure should gain a layer of redundancy and security. Intense System Segmentation within a single Virtual Machine (VM) should provide granular isolation to reduce the attack surface to a single file and/or single application, and reduce the ability of threats to virally propagate. End-point protection must also be customizable to address the specific needs of subsectors within individual Energy Sector Domains. Traditional virtualization techniques that use sandboxing have known, exploitable vulnerabilities. This is largely the result of the communication that traditional VMs require in order to perform sharing functions between applications and administrative requirements. Sandboxing also relies on binary decisions for processes and communication that might compromise security. Intense System Segmentation should allow communication between isolated environments to occur while eliminating any execution of code outside of an isolated environment. An Intense System Segmentation platform may use some of the tools of virtualization, such as a sealed hypervisor to provide protection of end-point resources, and sealed VMs to perform computing in intense isolation. Hypervisors are designed to streamline communication between a wide range of applications and processes, and utilize APIs and other communication entry points. A sealed hypervisor should block these communication entry points, for both the hypervisor and an attestable kernel. Maintaining the resiliency and continuous availability of the power grid should be one of the primary goals in creating a system segmentation platform. As this platform assumes that end-points will be penetrated, secure recovery, containment, and resiliency should be a focus of continued research. The inherent redundancy of hypervisor-driven segmentation can be utilized to enclose legacy systems and should allow customizable interoperability between the DHS-defined critical infrastructure sectors. An open platform that uses a secure computing architecture and leverages the tools of virtualization will enhance the resiliency of existing Energy Sector critical infrastructure. The use of virtualization has also been recognized as building block to implement resiliency through agility (a "moving target" paradigm). This can be used to increase uncertainty and cost to attackers. Thus, this research should help to leverage "moving target" paradigm in Smart Grid systems as well as improving security of Smart Grid legacy systems.