



Physical device recognition to the rescue

05/23/08

By Wilson P. Dizard III

Hardware fingerprinting technology migrates from fighting software piracy to shielding infrastructure

Sponsored By

Amid a kerfuffle over the resistance of the nation's electrical-grid control systems to cyberattack, a system known as physical device recognition (PDR) technology, first developed to foil computer software pirates, now is being shifted to the task of shielding electrical-grid control systems from cyberattack.

The cybersecurity risks linked to industrial-process control networks known as supervisory control and data acquisition systems came into focus during a May 21 hearing of the House Homeland Security subcommittee on cybersecurity. Information technology specialists agree that SCADA systems have become riskier in recent years because of their increasing interconnection with enterprise systems that ultimately link to the Internet.

PDR technology, developed by Uniloc USA, is being moved into the SCADA hardening world from its current home as a tool to prevent software pirates from exploiting intellectual property.

IBM and Oracle have licensed Uniloc PDR technology to protect their products, sources say. Uniloc also has used the technology to secure DVD content and protect road traffic signaling systems.

Uniloc's NetAnchor application uses PDR to carry out identity and access management functions for SCADA networks.

PDR technology relies on the internal electronic characteristics that distinguish individual hardware systems, even those manufactured to the same specifications, from one another. Those characteristics form a fingerprint that allows the PDR system to identify each system and authenticate it for connection to a SCADA network.

NetAnchor works with user authentication systems such as biometric controls to verify the identity of the equipment linking to a network and people who operate that equipment. NetAnchor uses a set of proprietary algorithms to generate the fingerprints.

"The Uniloc physical device fingerprinting algorithms allow the unique, reproducible identification of a device with an accuracy greater than $3.4 * 10^{38}$, allowing Uniloc to identify devices with more comparable accuracy than human DNA," the company said.

"When applied to NetAnchor CIS, the stage is set for this device-based authentication to stand as the leading access control solution for infrastructure security," the company said.

NetAnchor uses a server to carry out the fingerprinting function and a field unit to act as a gateway to the protected equipment. Devices outside the SCADA network that seek access must first establish their rights via a database of previously characterized, or fingerprinted, equipment. They then communicate via encrypted data links over a virtual private network. The application routinely rechecks the links' security via a challenge-and-response method during the connection session.

© 1996-2008 1105 Media, Inc. All Rights Reserved.