Improving Critical Infrastructure (CIP) Cyber Security

Jeffrey Robbins
President and CEO
LiveData, Inc.

LiveData Utilities
810 Memorial Drive
Cambridge, MA 02139
800.570.6211
info@livedatautilities.com
livedatautilities.com

Dramatically increased cyber threats[1] to critical infrastructure demand a need for a new level of cyber security to ensure operational reliability[2] and compliance with regulatory mandates[3]. Critical infrastructure (CIP) protection requires going beyond the standard information technology (IT) data protection provided by mainstream firewalls to include more robust technology designed to meet the different yet demanding needs of Operations Technology (OT)[4]. The protection of life, equipment and the environment, and service reliability place unique constraints on the barrier technology employed to maintain an effective electronic security perimeter and internally guarded network segments. Solutions need to be flexible and extensible to continually enable improving reliability, increasing responsiveness, while meeting or exceeding regulatory requirements in a cost-effective manner.

The global critical infrastructure protection market is forecast to exceed $100B by the year 2018[5]. Industry analysts estimate that in the US alone the market for protecting the electric power subset of critical infrastructure will reach $7.25B by the year 2020[6]. While traditional firewalls will play a role in the build-out, experts[7] agree that broader, more powerful solutions are required for effective network segmentation.

Firewalls are limited for this purpose in several respects:

1. They are typically not familiar with protocols used in ICS (Industrial Control Systems) and hence configuration generally requires ports to be opened with no packet level inspection

---

[1] SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat
Executive Order -- Improving Critical Infrastructure Cybersecurity
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] Reliability as defined by NERC:

- The system is controlled to stay within acceptable limits during normal conditions.
- The system performs acceptably after credible contingencies.
- The system limits the impact and scope of instability and cascading outages when they occur.
- The system's facilities are protected from unacceptable damage by operating them within facility ratings.
- The system's integrity can be restored promptly if it is lost.
- The system has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components. http://www.nerc.com/pa/Stand/Resources/Documents/AdequateLevelofReliability.pdf

[3] http://www.nerc.com/docs/standards/sar/CIP-005-5_clean_20111107.pdf

[4] http://www.smartgridnews.com/artman/publish/Business_Strategy/IT-OT-convergence-essential-definitions-and-important-trends-4044.html

[5] http://www.researchandmarkets.com/research/3m3xlw/critical

[6] http://etsinsights.com/reports/global-smart-grid-cybersecurity-systems-market-value-2012-2020/

[7] ICS-CERT, https://ics-cert.us-cert.gov/; NIST, http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm; EnergySec, http://www.energysec.org/

2. They generate voluminous logs but have no or little alert capability regarding intrusion when it comes to ICS protocols
3. Firewalls that deal with ICS protocols do so via lightweight add-ons that rely on relatively shallow probes of packets[8]

Data Diodes[9]:

Data diodes attempt to side-step the above problems by creating a unidirectional data flow, ensured by, in effect, physically severing the receive-side of a Transmit/Receive fiber pair. Unfortunately, since real-world ICS protocols are often of necessity bidirectional, the diodes must be deployed in pairs, with a proprietary non-routable protocol connecting the two diodes. This proprietary protocol must deliver reliably on ICS protocol latency and throughput requirements. Since the pair of diodes is wired in series, it represents a single-point-of-failure, raising the expensive prospect of FOUR diodes to achieve redundancy in service of high availability.

Even if the proprietary protocol and the costs of four diodes are acceptable, the fundamental non-end-to-end nature of the "server replication, not protocol emulation" approach means that the Supervisory Control and Data Acquisition (SCADA) system, for example, gets no feedback on the success or failure of data delivery to the upstream application. This can hobble the usefulness of connecting SCADA to other important systems such as an Outage Management System (OMS), where this lack of information concerning data delivery status can be costly. The unidirectional flow is at odds with OMS feedback to SCADA, depriving the SCADA system of additional system state knowledge otherwise known only to the OMS. In Operations, such lack of knowledge can be costly in terms of reliability and production, to be sure, but can also represent an increase in risk to human life when Operations is confronting the serious disruption of a bad storm or other major threats to production and delivery of power.

Network Guards (whitelisting):

Network guards, like the data diode, create a physical barrier and isolate networks without using a routable protocol. But by use of SELinux and other open and standard systems and protocols, guards can avoid the use of proprietary protocols. Additionally, by use of secured memory-to-memory operations, guards avoid the unavoidable latency of a pair of data diode boxes. Guards have historically relied upon manual and rules-based configuration to establish their whitelists.

---

[8] For example, the author is unaware of a standard firewall that can verify if an ICCP association attempt has the correct 'Bilateral Table Id', assuring proper configuration.

[9] http://www.securityweek.com/data-diodes-super-security-or-super-pain

New players are entering the whitelisting market, some with creative solutions to the documented challenges of manually configuring an application whitelist[10]. One solution uses an innovative machine learning approach to acquiring whitelist configuration. However, given that OT applications and ICS devices on OT networks typically lack strong authentication, standard IT authorization practices, and robust encryption, and furthermore can be sensitive to jitter in communication protocols, "server replication" must be accomplished via a trusted native protocol implementation. In replicating real-time data, a standard protocol is better than a proprietary protocol because:

1. Operations staff can support it
2. Avoids "format mismatch" issues at either side of the conversation (e.g. SCADA or OMS application)
3. Is compatible with the expectations of OT applications regarding message-passing behavior in terms of bandwidth, latency, jitter, and data quality attributes

This last point is a key element to cyber security success. Operations applications are often coded with very narrow timing constraints, and are sensitive to specific data quality attributes that impact their ability to share real-time data.

In an effort to logically partition the OT network from the rest of a utility's network, some analysts have positioned a specific logical function, the "Historian", as a store-and-forward repository for upstream users of OT data. While some Historian vendors understandably would like to blur the distinction between saving operational data in a file for subsequent analysis and sharing real-time grid state for operational management (including disaster response), grid managers responsible for applications such as OMS understand the distinction between historical and real-time data. Based on this distinction, an effective network barrier must be able to handle both historical file replication and real-time data replication. A successful solution should cater for this dual-role and provide a proven track-record in low latency, flexible and precise control of data flow, including both file-based traffic and real-time data protocol traffic.

In addition to providing the appropriate level and layers of security, solutions suitable for critical infrastructure security must be fluent in the languages that control the power network. This fluency, combined with up-to-date model-awareness, will allow the system to enforce rules that check both syntax and "right operation only at the right time", without incurring the pain of manual whitelisting, or flying blind due to one-way-only communication.

[10] http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599

Evaluating Cyber Security Solutions for Critical Infrastructure Systems:

Grid operators need to upgrade their cyber defenses against damaging cyber attacks, while maintaining (if not improving) safety, reliability, and compliance. Traditional firewalls have been shown to interfere with Operations Technology (OT) and at the same time lack the ability to provide the manageable whitelists required. Grid operators need to be able to easily manage, maintain, and update systems to meet current and future regulatory mandates, as well as react to and deflect attacks as they continually evolve.

A Checklist of Features to Look For:

- Viable OT protection against external and internal cyber threats
- Reliable and responsive enforcement of "right command only at the right time"
- Meet or exceed NERC CIP 5 requirements (segmentation, whitelisting, auditing)
- Purpose-built device to monitor a specific ICS protocol
- Devices for most popular ICS protocols – ICCP, DNP, Modbus, & OPC
- In-memory grid state to arbitrate access to critical points
- Rule-base for abnormal communication & related alert
- Scalable solution to protect and manage multiple devices and complex rules
- Central command center to manage all these devices for suspicious activity, alerts
- Provides deep protocol inspection to monitor communication and ensure authorized access to OT data.
- Provides for ICS protocol-specific solutions to monitor suspicious activity/data from field devices within OT network.
- System has the ability to maintain an in-memory representation of the grid's state, so it can detect and flag suspicious operational commands.

Appendix A: Cyber Security Threats

Authorization violation: Access by an entity lacking proper access rights.

Bypassing controls: Exploitation of system flaws or vulnerabilities by an authorized user in order to acquire unauthorized privileges.

Denial of service: Deliberate blocking of legitimate access to devices and/or information.

Eavesdropping: Acquisition of information flows, sometimes by "listening" to radio or wireline transmissions, sometimes by analyzing traffic on a local area network.

Illegitimate use: knowingly or unknowingly intruding on system resources.

Indiscretion: Indiscriminate opening of information files or access to field devices.

Information leakage: Unintentional provision of information to a third party.

Integrity violation: Messages and the computer infrastructure subjected to unauthorized modification or destruction.

Intercept/alter: Intercepting and altering information flows, usually by accessing devices and modifying data.

Masquerade: Posing as an authorized user on a network, the most common method used by hackers to gain access to networks, often enabled by having other users' passwords. A masquerader can view secret information, alter or destroy data, use unauthorized resources, and deny legitimate users access to services.

Replay: Use of information previously captured (without necessarily knowing what it means).

Repudiation: Denial by an entity that it undertook some action such as operating a device or receiving information.

Spoof: Occurs when a user or application believes it is using a legitimate computer service, while actually performing some different function.

About LiveData Utilities

LiveData Utilities is the trusted source for operations technology data integration and visualization. Our smart grid solutions deliver operational intelligence to enable confident real-time management of power grid assets for critical infrastructure network segmentation and protection; ISO connectivity; SCADA, OMS, and DMS real-time state monitoring, control, and communication; demand response aggregation; visualization; and data analytics. Founded in 1991, LiveData is headquartered in Cambridge, MA. For more information, visit www.livedatautilities.com.