Data Diodes in Support of Trustworthy Cyber Infrastructure

Hamed Okhravi[*]
University of Illinois at Urbana-Champaign
1308 West Main St.
Urbana, IL
okhravi@mit.edu

Fredrick T. Sheldon
Oak Ridge National Laboratory (ORNL)
One Bethel Valley Rd, M/S 6418
Oak Ridge, TN
sheldonft@ornl.gov

ABSTRACT

Interconnections between process control networks and enterprise networks has resulted in the proliferation of standard communication protocols in industrial control systems which exposes instrumentation, control systems, and the critical infrastructure components they operate to a variety of cyber attacks. Various standards and technologies have been proposed to protect industrial control systems against cyber attacks and to provide them with confidentiality, integrity, and availability. Among these technologies, data diodes provide protection of critical systems by the means of physically enforcing traffic direction on the network. In order to deploy data diodes effectively, it is imperative to understand the protection they provide, the protection they do not provide, their limitations, and their place in the larger security infrastructure. In this work, we briefly review the security challenges in an industrial control system, study data diodes, their functionalities and limitations, and propose a scheme for their effective deployment in trusted process control networks (TPCNs.)

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; B.4.1 [**Input/Output and Data Communication**]: Data Communications Devices

General Terms

Security

Keywords

Data Diodes, Trusted Process Control Networks, Industrial Control Systems

1. OVERVIEW OF PCNS AND SECURITY CHALLENGES

Figure 1 illustrates a typical process control network (PCN) architecture with paired firewall. In this architecture, the PCN contains the low level control devices such as programmable logic controllers (PLCs), remote terminal units (RTUs), master terminal unit (MTU), and the operator console. The enterprise network often contains the workstations and high level management consoles. The data historian sits in the demilitarized zone (DMZ) of the firewalls and acts as an intermediary between the PCN and EN. In fact, to protect the PCN from attacks and breaches going through the EN, status data is collected from the historian and not from the PCN directly.

Protecting PCNs often faces several challenges. Firewall configuration errors may result in unwanted traffic going to the PCN or legitimate traffic being dropped. In fact a study by Wool [15] shows that 80% of firewall rule sets allow any service on inbound traffic and insecure access to firewalls. Moreover, a firewall maybe bypassed by an attacker using encrypted tunnels (e.g. VPN) or unsecured out-of bound communication (e.g. dial-up maintenance connection.) Vulnerable end devices also pose a threat to the security of PCNs. Software/configuration bugs in the control devices may be exploited by an attacker to gain illegitimate access to the system or change the configuration of the critical components. Unsecured physical access to any part of the network (unsecured Ethernet ports) may also result in a benign or malicious damage to the PCNs. In addition, untrusted (rogue) devices or users may enter the network and breach its security. Finally, all of the above mentioned mechanisms may introduce malware (worms and viruses) to the critical systems.

2. DATA DIODES

Data diodes provide a physical mechanism for enforcing strict unidirectional communication between two networks. They are often implemented by removing transmitting component from one side and receiving component from another side of a bidirectional communication system (e.g. a fiber optic system with TX capability in only one side and RX capability in the other side.) Data diodes can only send information from one network (a.k.a the "low" network) to another network (a.k.a the "high" network.) The high network often contains data with higher classification level than the low network. Figure 2 illustrates two networks connected by a data diode.

2.1 Protection Provided

Data diodes can provide strong confidentiality from the high network to the low network; i.e. provided that the unidirec-

[*] The author is currently with MIT Lincoln Laboratory.

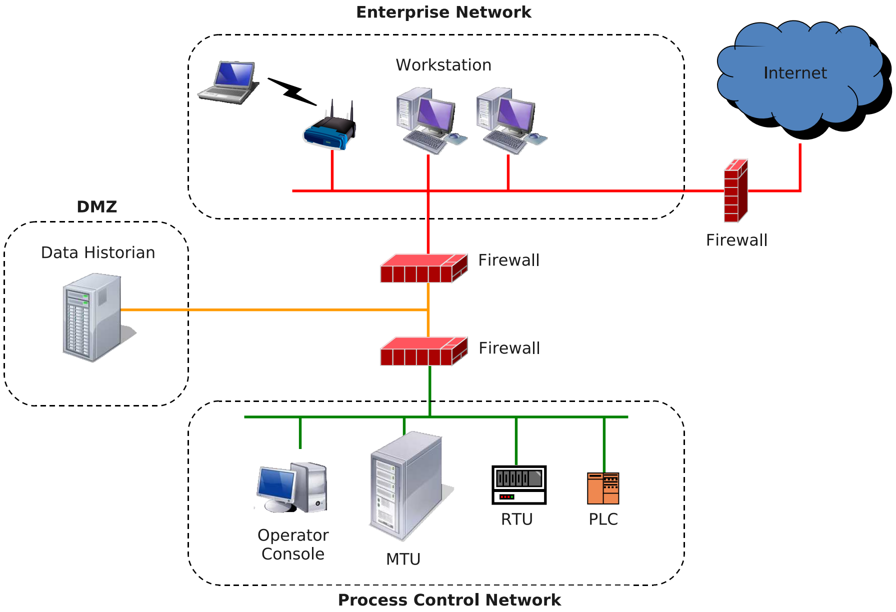

Figure 1: A typical paired-firewall industrial control system.

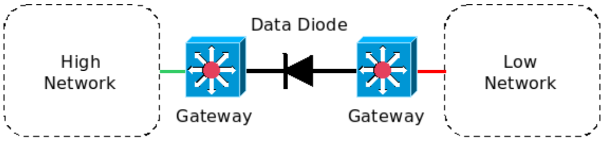

Figure 2: Two networks connected by a data diode.

tional connection is the only communication link between these two networks, information can flow from low to high, but there is no backflow of data. In a dual fashion, data diodes can provide strong integrity from the low network to the high network; i.e. a malicious component in the high network cannot corrupt data or perform network-based attacks on the low network (availability).

2.2 Protection Not Provided

It is sometimes claimed that data diodes protect the high network against cyber attacks. This, in fact, is not correct. Many cyber exploits do not require a session or bidirectional communication. Often fast propagating worms or malware need just one packet of data to infect a machine. Self expanding malware or quine programs [7] even limits the number of bytes required in the packet [13].

Moreover, in industrial control systems, the process control network is the critical component of the system for which availability and integrity are important properties. If the process control network is connected to the “high” side, the data diode does not protect it against breaches from the low network.

2.3 Limitations

A major limitation of the data diode is that it does not work with the standard TCP/IP protocols. It needs proprietary unidirectional protocols that do not require acknowledgments. On both sides of a data diode, gateways translate unidirectional protocols to standard bidirectional protocols to connect the diode to the rest of the network [4]. However, more high-end products [3] also accept TCP or UDP packets as input. Data diodes can be used to enhance security, but they are by no means even a nearly complete solution. They have to be placed carefully in conjunction with other defensive mechanisms.

2.4 Implementation

Data diodes are often implemented using serial links (RS-232) or optical fiber. In the serial link implementation, one of the two data cables (from high to low) is removed. In optical data diodes, the transmitter of the high network and the receiver of the low network are removed.

A major disadvantage of the RS-232 implementation is that in addition to data lines, there are control lines defined in the standard along which data can potentially flow back to the low network. Hence, optical fiber is the preferred implementation of data diodes.

3. TRUSTED PROCESS CONTROL NETWORK WITH DATA DIODES

A TPCN architecture [12] deploys trusted network (TN) [2, 1] technology to establish trust in industrial control systems. It uses information about the hardware and software states of devices in admission and access control decisions. When a device first joins the network, its hardware and software are checked; based on these checks, the appropriate access control rules are applied dynamically to the user, device and traffic. A TPCN architecture uses existing standards, protocols, and hardware devices to extend the concept of "trust" to the network architecture.

A TPCN has the following components:

- Client device: Every client device must be evaluated prior to admission to a TPCN.
- Network Access Device (NAD): All connectivity to a TPCN is implemented via a NAD, which enforces policy. NAD functionality may exist in devices such as switches, routers, VPN concentrators and wireless access points.
- Authentication, Authorization, and Access Control (AAA) Server: maintains the policy and provides rules to NADs based on the results of authentication and posture validation.
- Posture Validation Servers (PVSs): evaluate the compliance of a client before it can join a TPCN. A PVS is typically a specialization for one client attribute (e.g., operating system version and patch or virus signature release).
- Posture Remediation Servers: provide remediation options to a client device in the case of non-compliance.
- Directory Server: authenticates client devices based on their identities or roles.
- Other Servers: These include trusted versions of Audit, DNS, DHCP and VPN servers.

A TPCN architecture is presented in Figure 3. A client device intending to join the network communicates its request to the NAD. The NAD establishes the client device's identity using EAP over the 802.1x protocol and sends the results to the AAA server using the RADIUS protocol. The AAA server returns a list of posture validation requirements and the addresses of the appropriate PVSs. The client then validates its posture with each of the PVSs. If the client is in compliance, the results are sent to the AAA server using the HCAP protocol. On the other hand, if the client lacks one or more requirements, the appropriate posture remediation servers suggest remediation actions to the client. The directory server determines the client's group or role. Given all the results from the PVSs and the directory server, the AAA server determines the set of rules that apply to the client's access and traffic and sends them to the NAD for enforcement.

From this point on, the client is permitted to communicate via the NAD and all its activities are monitored for policy compliance. The policy held by the AAA server is in the form of an authentication requirement and a list of posture validation requirements.

When a client device joins the network, a NAD communicates with an AAA server on behalf of the device. The AAA server authenticates the device and provides rules based on the device's security postures to the NAD. From this point on, the NAD enforces the policy on all ingress and egress traffic to/from the device. For example, an RTU with valid firmware is allowed to communicate with the historian; all other traffic is blocked. Okhravi and Nicol [12] provide two examples to further clarify the workings of a TPCN. They also describe methods to enhance availability of TPCNs and limit the number of configuration errors.

A TPCN addresses many of the security challenges by providing defense-in-depth and extending trust to the process control devices [11].TPCNs build a security infrastructure for mission critical systems. Data diodes can be used to enhance TPCN protection by strictly limiting traffic at some sensitive points.

An important component of the TPCN network that can benefit from data diodes and tolerate their limitations is the data historian. The firewalls are often configured to drop any traffic going from the data historian to the PCN. If a data diode is placed between the historian and the PCN, the critical control devices can still push their status data to the DMZ while no traffic can flow back. Another diode may also be placed between the DMZ and EN to protect the integrity of the historian. Note that in both cases the "high" end of the diode is connected to the less critical components. This protects the PCN against attacks from EN or DMZ, granting integrity and availability. The confidentiality of the data sent to historian is arguably less important than protecting the PCN.

4. RELATED WORK

Kang, et al. [9] first designed and implemented a network device, *network pump*, for limiting convert back flow of data across the network. Network pump keeps the communication bidirectional, but it queues and sends the acknowledgments at probabilistic times. Stevens and Pope [10] discuss different implementations of data diodes and their assurance levels and limitations. Jones and Bowersox [8] propose the use of data diodes in secure data exports for voting systems. Finally, Roach [14] demonstrates the application of data diodes in aircraft instrumentation systems. To the best of our knowledge, we are the first to propose the application of data diodes in industrial control systems and develop a security infrastructure based on TPCNs for effective deployment of data diodes in process control applications.

5. CONCLUSION AND FUTURE WORK

Data diodes can offer some protection in the expense of imposing some limitations to the system. To effectively deploy them in a system, it is important to fully understand their functionalities and limitations. They cannot offer a comprehensive security solution, yet they can enhance the security of the system if used with care. A TPCN presents a trusted infrastructure for industrial control systems that can remedy many of the security issues. Data diodes can be placed

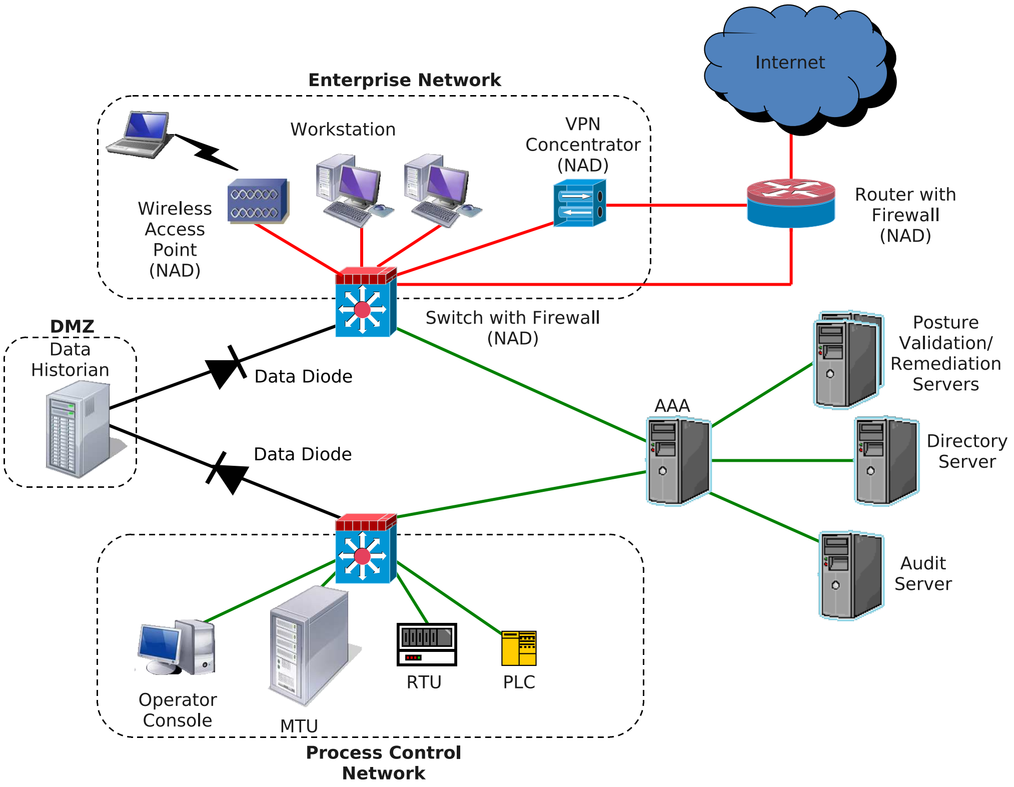

Figure 3: A TPCN with data diodes.

in sensitive places in a TPCN to protect the integrity of the control components and enhance the availability of the system. Based on our work on NAD rule conflicts [12], we plan to develop an algorithm to distribute firewall rules in the presence of data diodes in order to minimize rule conflicts [6] and implement a prototype on top of our testbed [5].

6. REFERENCES

[1] Network Admission Control (NAC). Technical overview, Cisco Systems, Inc., 2005.

[2] Getting started with Cisco NAC network modules in Cisco access routers. Technical manual, Cisco Systems, Inc., 2007.

[3] Interactive Link Data Diode Device. Manual, BAE Systems, 2010.

[4] Waterfall's Unidirectional Security Gateways. Manual, Waterfall, 2010. http://www.waterfallsecurity.com/technology/.

[5] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol. SCADA cyber security testbed development. In *Proceedings of the 38th North American Power Symposium (NAPS 2006)*, pages 483–488, 2006.

[6] A. Hari, S. Suri, and G. Parulkar. Detecting and resolving packet filter conflicts. In *Proceedings of IEEE INFOCOM*, pages 1203–1212, 2000.

[7] D. R. Hofstadter. *Godel, Escher, Bach: An Eternal Golden*. Basic Books, Inc., New York, NY, 1 edition, 1979.

[8] D. W. Jones and T. C. Bowersox. Secure data export and auditing using data diodes. In *EVT'06: Proceedings of the USENIX Electronic Voting Technology Workshop 2006*, pages 4–4, Berkeley, CA, USA, 2006. USENIX Association.

[9] M. H. Kang, I. S. Moskowitz, and S. Chincheck. The pump: A decade of covert fun. In *ACSAC '05: Proceedings of the 21st Annual Computer Security Applications Conference*, pages 352–360, Washington, DC, USA, 2005. IEEE Computer Society.

[10] S. M. and P. M. Data Diodes. Technical report - dsto-tr-0209, Electronics and Surveillance Research Laboratory (DSTO), 1995.

[11] H. Okhravi and D. Nicol. Applying trusted network technology to process control systems. In E. Goetz and S. Shenoi, editors, *Critical Infrastructure Protection II*, pages 57–70. Springer, Boston, MA, 2 edition, 2008.

[12] H. Okhravi and D. Nicol. Application of trusted network technology to industrial control networks. *Elsevier International Journal of Critical Infrastructure Protection (IJCIP)*, 2(3):84–94, 2009.

[13] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Is your cat infected with a computer virus? In *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 169–179, 2006.

[14] J. Roach. The architecture of aircraft instrumentation networks. In *Proceedings of the International Telemetering Conference (ITC 2007)*, 2007.

[15] A. Wool. A quantitative study of firewall configuration errors. *Computer*, 37(6):62–67, 2004.