UNIDIRECTIONAL SECURITY GATEWAYS: STRONGER THAN FIREWALLS

Andrew Ginter, Waterfall Security Solutions, New York, USA

Abstract

In the last half decade, application integration via Unidirectional Security Gateways has emerged as a secure alternative to firewalls. The gateways are deployed extensively to protect the safety and reliability of industrial control systems in nuclear generators, conventional generators and a wide variety of other critical infrastructures. Unidirectional Gateways are a combination of hardware and software. The hardware allows information to leave a protected industrial network, and physically prevents any signal whatsoever from returning to the protected network. The result is that the hardware blocks all online attacks originating on external networks. The software replicates industrial servers to external networks, where the information in those servers is available to end users and to external applications. The software does not proxy or emulate bi-directional communications protocols. Industrial security standards and regulations are evolving to reflect this strong alternative to network firewalls.

INTRODUCTION

Large physics experiments may face safety concerns including: handling radioactive materials and toxic materials and operating dangerous equipment such as high-powered lasers and powerful electromagnets. These experiments may also face reliability concerns including: disruption of costly experiments due to mis-operation of experimental apparatus and possible damage to costly equipment as a result of mis-operation or other errors.

These large research experiments constitute large, dangerous physical processes – in that sense similar to large, dangerous industrial processes used world-wide to automate production of a wide variety of goods and services. Both these large experiments and large industrial processes rely on a variety of both commercial and custom industrial control system components to operate these physical processes safely and reliably.

Cyber security has been a topic of concern for industrial control systems for over a decade. Cyber threats range from conventional viruses and botnets impairing operations to the point that costly physical processes must be shut down while control system components are repaired, to targeted or advanced threats to specific facilities due to “hacktivists,” terrorists and even nation-state militaries and intelligence agencies.

Large physics experiments face all of these threats, as well as additional threats unique to these experiments. For example, visiting researchers may not be familiar with removable media controls or limitations as to which networks visiting laptops may safely be connected. In addition, industrial sites generally do not transmit extremely detailed information regarding the operation of the physical process to external networks, but such transmissions may be essential to the research and educational missions of large experiments. It is very difficult to carry out such communications via conventional firewalls without introducing the risk of cyber compromise to the experiment’s control systems.

This paper introduces unidirectional security gateways as a strong alternative to firewalls, and describes how the gateways are being used to secure industrial control systems, as well as how industrial control systems standards and regulations are evolving to reflect the security offered by hardware-enforced unidirectional security gateways.

UNIDIRECTIONAL SECURITY GATEWAYS

Unidirectional security gateways are a combination of hardware and software, designed to securely integrate a variety of external applications with industrial control systems components, by replicating servers from industrial networks to external networks [1].

Gateway Hardware

While commercially available unidirectional communications components may be bundled in a variety of ways, the majority protect industrial systems through optical isolation. A typical hardware implementation consists of a pair of network appliances joined by a fibre-optic cable. The “TX” or “transmit” appliance contains a fibre-optic transmitter, and the “RX” or “receive” appliance contains a fibre-optic receiver. Unlike conventional fibre-optic communications components which contain both transmitters and receivers, the TX appliance does not contain a receiver, and the RX appliance does not contain a transmitter.

The equipment is usually oriented to transmit information out of the control system network into an external network, or directly out to the Internet, without any risk of any cyber attack or any other signal whatsoever returning into the control system to put safe and reliable operation of the physical process at risk. When the unidirectional gateway hardware is deployed as the only online connection between the control system network and any external network, the control system network is effectively protected against any online attack originating on an external network. The gateways eliminate this threat vector entirely.

The gateway hardware is similar to “data diode” hardware [2], which is used to allow information to pass into classified military and government networks, without leaking any sensitive information out of those networks. Unlike data diodes, which tend to be accompanied by comparatively simple file transfer and Internet Protocol

Copyright © 2014 CC-BY-3.0 and by the respective authors

ISBN 978-3-95450-139-7

(IP) proxying application software, unidirectional gateways are software-intensive. The term unidirectional gateway is being used in international standards and other publications to describe the combination of hardware and software which replicates industrial servers to external networks while protecting the safety and reliability of those industrial networks.

Gateway Software: Server Replication

Unidirectional gateway software replicates industrial server applications from industrial networks to external networks. For example, industrial networks routinely employ process historians: databases optimized to manage time-sequenced data. To deploy the gateways to replicate a historian database server, a control system site first ensures that a historian database server is deployed on the control system network, and a second historian server is deployed on the external network, see Fig. 1.

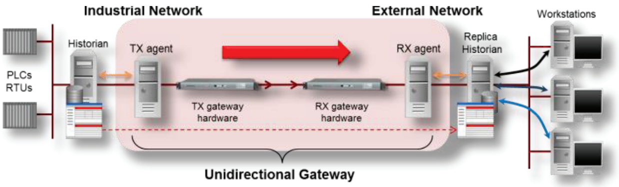

Figure 1: Historian replication.

Unidirectional gateway "agent" software is then deployed on two machines: a TX agent host inside the industrial network, and an RX agent host on the external network. The agent software on the industrial network connects to the industrial historian database and issues queries to the database. Historical data retrieved from the industrial database is sent across the unidirectional gateway hardware to the RX agent host on the external network. The RX agent registers as a client of the replica historian database, and issues insert requests to that database, asking the database to store all of the time-stamped data the RX agent receives from the industrial network.

Users and applications on the external network which need access to the historical data all access the replica historian. Any attacks which may be launched against the replica or any performance problems which may arise in the replica are immaterial to the industrial process. The protected control system is unable to determine so much as whether the RX gateway is turned on, much less whether any attack might be in progress on the external network.

Device Emulation

When the information which must be moved to an external network is stored in control devices or other servers whose programming or communications interfaces do not have "insert" semantics, device emulation may be necessary. In this case, the TX agent queries the original device or server for data, or receives that data through some other means, such as SNMP traps or SMTP requests. The data is then sent across the gateway hardware to the RX agent. The RX agent then tends to emulate the original industrial device/server through the use of standard protocols or libraries.

For example, many physical-process monitoring and control devices communicate via the open Modbus protocol. To replicate / emulate Modbus devices, the TX agent queries these devices for all of their data, and sends that data to the RX agent via the gateway hardware. The RX gateway then emulates the original device by storing the data temporarily, and responding to Modbus queries using the received data, as if the RX agent were the original Modbus device. Note that it is not the Modbus protocol which is being emulated here – industrial protocols tend to be used in the form of standard libraries. It is the *device* which is being emulated, by responding to Modbus queries as if the RX agent were the original device.

Apparently Bi-Directional Requirements

Unidirectional gateways are deployed routinely in circumstances with requirements which security practitioners might regard as strongly bi-directional [3]. For example, remote screen view technology can take pictures of the monitor of equipment in the protected network and send those pictures to external viewers in real time. When remote support is needed, remote vendors and other support personnel watching these screen captures can provide verbal advice via telephone to personnel at the site to help diagnose and correct problems. Or a dedicated "operations" Wide Area Network (WAN) can be used to provide remote support from a central engineering site, a site which is normally thought to require bi-directional communications. Provided the engineers at the central site have direct access to the operations WAN, and provided the sole connection between the operations WAN and any external network is still unidirectional, the operations WAN still enjoys unidirectional protection from online attacks originating on external networks.

Industrial Applications

Unidirectional security gateways are used in a wide variety of industrial applications. At this writing, all American nuclear generators use unidirectional gateway technology to separate safety and control networks from corporate/business networks. Nuclear generators in Spain and Korea are adopting the technology as well. The largest installed base for unidirectional gateways though, is conventional power generation, including coal-fired, hydro, gas turbine, combined-cycle, and thermal solar generators.

The technology is used in a wide variety of other industries as well, including refineries, chemical plants, municipal water and wastewater treatment systems, offshore oil and gas drilling and production platforms, and oil and natural gas pipelines.

Again, these applications are similar to applications in large physics experiments in that the installations represent large investments and are susceptible to damage

Copyright © 2014 CC-BY-3.0 and by the respective authors

ISBN 978-3-95450-139-7

and outages through misuse or cyber-sabotage, and the installations manipulate quantities of toxic materials, flammable materials, and radioactive materials sufficient to pose a threat to workers at the site, and sometimes to the public at large.

INDUSTRIAL SECURITY STANDARDS

Unidirectional security gateways are available from a variety of security product vendors and have been installed in a significant number of industrial settings in a variety of industries. All of these criteria are necessary to qualify the technology for inclusion industrial cyber security standards, guidance and regulations, as those documents are revised.

NERC CIP V5

At this writing, version 5 of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards has been submitted to the Federal Energy Regulatory Commission for approval [4]. Version 5 is the first version of the standard which directly addresses unidirectional gateway technology.

The standard includes the definition of External Routable Connectivity (ERC) as: "The ability to access a BES Cyber System that is accessible from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a ***bi-directional*** routable protocol connection" [emphasis added]. Since unidirectional security gateways are by definition not bi-directional, the gateways do not qualify as ERC. As a result, medium-impact assets under the V5 CIP standard are exempted from some 37 of the 103 requirements in the standard – exempted from those requirements which apply only if a medium-impact asset is accessible via ERC. In effect, the CIP V5 standard reduces compliance obligations and costs for sites deploying unidirectional security gateways instead of firewalls.

ISA SP-99 / IEC 62443

The International Society of Automation (ISA) in conjunction with the International Electrochemical Commission (IEC) are defining more than a dozen industrial security standards – the exact number varies over time as progress is made on the standards. The most recently published standard ISA/IEC 62443-3-3 "Security for industrial automation and control systems, Part 3-3: System security requirements and security levels" mentions unidirectional security gateways as an alternative to firewalls in all examples of network cyber-perimeter protections [5]. Additional standards and technical reports are in progress. This author is the co-chair of one of these committees and a reviewing member of many others and can attest to the fact that unidirectional gateways are being considered in many of the draft standards.

NEI 08-09 & NRC 5.71

The Nuclear Energy Institute (NEI) and the Nuclear Regulatory Commission (NRC) have issued cyber-security guidance and standards/regulations documents, respectively [6] [7]. The two documents are very similar, which is not surprising given that largely the same set of individuals developed both documents.

Each document provides a long list of requirements for nuclear generators which expose safety networks and control networks to external networks via firewalls. Each document provides a very short list of requirements for sites which protect safety networks and control networks with unidirectional gateway technology.

CONCLUSIONS

Unidirectional security gateways are being deployed routinely in some industries to protect control system networks from online attacks from external networks. Industrial control system standards and regulations are evolving to include unidirectional gateways as an alternative to firewalls. The gateways are being deployed routinely even to protect network connections which on the surface appear to have strong bi-directional communications requirements. Industrial security standards are evolving to include mention of this alternative to firewalls, and in some cases to offer regulatory encouragement for the use of unidirectional gateways. Practitioners responsible for securing industrial control system networks as well as control system networks for large physics experiments are advised to become familiar with this alternative to conventional firewalls.

REFERENCES

[1] L. Frenkel et al., "Experience with Unidirectional Security Gateways Protecting Industrial Control Systems," CRITIS'12, September 2012.

[2] M. W. Stevens, "An Implementation of an Optical Data Diode," Australian Department of Defence, May (1999); http://www.dsto.defence.gov.au/publications/2110/DSTO-TR-0785.pdf

[3] L. Frenkel, "Advanced Protection for Advanced Threats: Securing Turbine Management Connections," Advanced Computing Solutions 2011 Industrial Control Systems Cyber Security Conference, September 2011; http://www.waterfall-security.com/category/resources/

[4] G. W. Cauley et al., "Petition of the North American Electric Reliability Corporation For Approval of Critical Infrastructure Protection Reliability Standards Version 5," January (2013); http://www.nerc.com/news/Headlines%20DL/Final_Petition_CIP_V5_01-31-13%20and%20Exhibits%20A-E.pdf

[5] International Society of Automation, "ANSI/ISA‑62443‑3‑3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels," August 2013.

[6] Nuclear Energy Institute, "NEI 08-09 [Rev. 6] Cyber Security Plan for Nuclear Power Reactors," April 2010.

[7] U.S. Nuclear Regulatory Commission, "Regulatory Guide 5.71 Cyber Security Programs for Nuclear Power Plants," January 2010.

Copyright © 2014 CC-BY-3.0 and by the respective authors

ISBN 978-3-95450-139-7