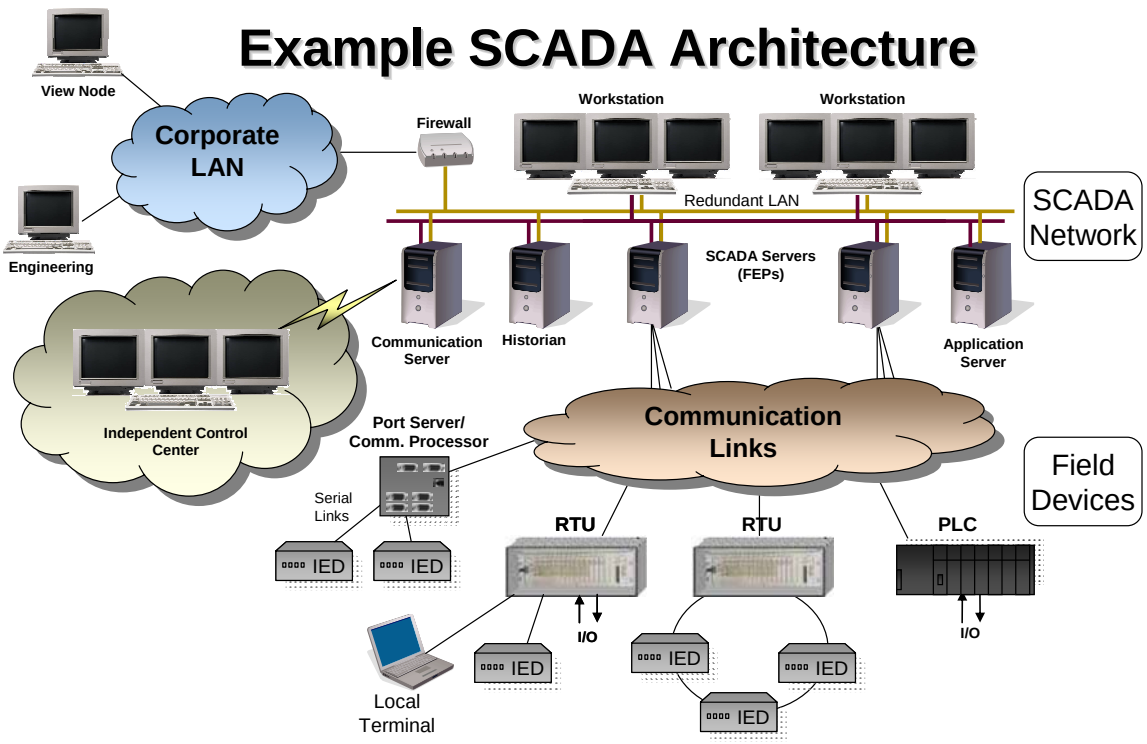
The Role of Authenticated Communications for Electric Power Distribution
Pacific Northwest National Laboratory, U.S. Department of Energy

Position Paper for the National Workshop – Beyond SCADA:
Networked Embedded Control for Cyber Physical Systems (HCSS-NEC4CPS)
November 8-9, 2006

Background

"Control Systems are the "brains" of the control and monitoring of the bulk electric system and other critical infrastructures, but they were designed for functionality and performance, not security. Most Control Systems assume an environment of complete and implicit trust."[1] This quote from the North American Electric Reliability Council (NERC) Control Systems Security Working Group (CSSWG) describes the control system environment extremely well. The devices, protocols and communication media do not support the ability to adequately prevent cyber attacks against our critical infrastructure. In the following sections we will explore each of these areas in more detail, identify the requirements for a solution, and present a path forward for building trust into SCADA / control system communication.

Environment



The above diagram depicts a typical Electric Power SCADA system and connections to other networks such as those belonging to backup control centers, the corporate network, and field devices. The focus of this paper and the authentication technology is on the communications links between the SCADA network and field devices.

Hundreds of SCADA protocols exist today, and the following table contains a sample showing the variety of methods used to indicate message start and end. Some of these protocols are capable of supporting more than just telemetry and control functions. DNP3, for example, allows for the uploading of a new firmware version via a file transfer as well as warm or cold rebooting of the remote device.

Protocol	Message start & stop	Notes
Modbus RTU	Timing based	Used heavily in water/oil sectors
Modbus ASCII	Special characters	
DNP3	Length based	Object oriented
Conitel	Bit-based	Original protocol developed in 1967 by GTE
UCA / IEC 61850	Length based	Plug & play, device interrogation

SCADA protocols were designed with noisy serial communication environments in mind, and the use of cyclic redundancy codes (CRC), or similar technology, is present for error detection and correction. The sender of the message will calculate the CRC and append it to the message. The receiving device will calculate the CRC for the message and compare it to the value received with the message. If a bit was flipped during transmission, the CRC indicates an error occurred during transmission.

Another common characteristic for SCADA protocols is the inability to provide authentication or validation services. This is the primary reason why SCADA systems assume a level of implicit trust. For example, when a message is received by an RTU, the source of the message is checked, and if that source is known, the request is enacted. No questions asked. Protocol trends are a concern as well. In the electric distribution world, DNP3 is becoming the de facto standard, and DNP is an open standard. Information on message structure and vulnerabilities are appearing on the Internet. Worse, information on how to attack DNP and other SCADA protocols is beginning to surface at black hat events such as Toorcon.

In addition to protocol vulnerabilities, the communication links shown in the diagram are subject to man in the middle attacks. Electric distribution SCADA systems are geographically dispersed, and it is common for the connections to remote facilities or devices to be made over dial up, leased lines, or SCADA radios. While the specific attacks for these communication methods differ, each can be compromised. For example, SCADA radio is a strong signal, typically 1 watt. At that power, the signal can travel 15 miles or more. This provides ample opportunity for an adversary to break in without being detected.

Requirements

To guide research and development activities for a solution to the protocol and communication vulnerabilities previous expressed, an advisory board of grid operators, asset owners, and industry consultants was formed. High level requirements expressed by the advisory board are listed below:

- Need to provide authentication and validation without encryption
- Introduced latency needs to be minimal
- Embed technology onto FEP and end devices
- Support legacy systems
- Cannot impact safety
- Cost cannot exceed $250 for legacy system support
- Each remote site needs to have their own key
- Provide IDS capabilities
- Message validated before enacted

- Need to fit into existing telemetry environment without modification
- Traffic will be authenticated and validated in both directions
- Start with DNP3
- Interface with standards bodies after the technology is proven

To meet these requirements, three different solutions were developed. The first is a suite of software applications that reside on the SCADA master/FEP to authenticate traffic before the traffic is placed onto the communications channel. Two “bump in the wire” solutions were also developed to support legacy systems. One bump in the wire solution is software that resides on an industrial computer that can be placed between the modem and remote device or between the FEP and its modem. The other bump in the wire solution is a low cost micro controller that runs a scaled down version of the code for legacy environments.

Path forward

The authentication technology was successfully field tested in the production environment at CenterPoint Energy in May and June 2006. The next steps are to build upon that effort by working with the DNP Users Group and IEC Technical Committee 57 Working Group 15 to build authentication, validation, key update, and event reporting into the DNP standard. Simultaneously, work with DNP software vendors to transfer the technology out of the laboratory and into industry so complete end to end protection of communication can be implemented. Finally, target other protocol so implicit trust can be removed from the SCADA systems for other sectors.

References

1) NERC Control Systems Security Working Group charter, http://www.nerc.com/~filez/csswg.html