

# Secure Historian Access in SCADA Systems

Dylan McNamee, Trevor Elliott  
Galois, Inc. Portland, Oregon  
{dylan,trevor}@galois.com  
June 30, 2011

## Executive Summary

Securing SCADA infrastructure from cyber attacks is a critical task, and is an active area of investigation among a broad group of stakeholders. This white paper suggests an approach to a specific aspect of SCADA security - making Historian data available to users and systems outside the protected SCADA enclave. To do this, we propose using a research prototype of the “Trusted Services Engine” (TSE), developed at Galois to provide high assurance, cross-domain data sharing between networks of different classification levels, but configured to facilitate one-way information flow. This paper describes the context of the problem, the approach we propose, and some next steps: identifying a partner team familiar with SCADA security issues and to investigate the viability and benefits of this approach. We believe that using the TSE to provide remote access to Historian data could increase the trustworthiness of the isolation between untrusted networks and SCADA enclaves. We describe the advantages of using a TSE over a data diode solution. We seek interested stakeholders and partners, and are interested in evaluating the effectiveness of this approach, perhaps through test deployments in an SCADA system testbed.

**Keywords:** SCADA, Information Assurance, Security

## 1 Background: Growing Threats to SCADA Infrastructure

SCADA stands for *stands for supervisory control and data acquisition*. SCADA systems are *cyberphysical* in that they are computer systems that interoperate with machines, actuators or sensors that interact with the physical world. SCADA often applies to industrial control systems that interact with critical infrastructure, such as power generation and distribution, traffic lights, railroads, elevators, etc.

Two well-established trends are coming to a troubling intersection. The first trend is of critical systems coming on-line. This is evident in the increasing use of internet infrastructure (hardware and protocols) to build and control SCADA systems. The second trend is the increasing awareness among adversaries that attacking computer network assets can be as, or more, effective than attacking physical ones. This awareness has brought increased expertise in compromising computer security mechanisms. The intersection of these trends is that the impact of a successful cyberattack continues to grow. Money, time, and lives are all at risk if a SCADA system is compromised and manipulated by an adversary. Current “best-of-practice” security measures are being promoted and implemented at SCADA sites [Stouffer et al. 2008], however even these may not be nearly sufficient to protect such a system from a determined and/or well-funded adversary. New measures need to be invented and deployed.

## 2 Challenge: Secure Access to Historian Data

This paper proposes to leverage a technology developed at Galois for the Department of Defense (DoD) towards securing one key aspect of a SCADA system. That aspect is making data available from

the Historian to users and systems outside the trusted SCADA enclave, as shown in Figure 1. The Historian is a subsystem that keeps an audit-log of all the activities on a SCADA network. The channel, from the Historian inside the SCADA network to external systems that need remote access through the Internet, is usually protected by one or more firewalls configured to allow traffic only outward, and to prevent hackers from tampering with anything inside the SCADA network. Firewalls are useful for preventing many kinds of attacks, but themselves are subject to attack, and such attacks have occurred [Kamara et al. 2003]. The penetrate and patch approach, which is often appropriate for commercial firewalls [Cisco Systems, Inc. 2007], is inappropriate for protecting such critical assets from zero day attacks, in which an attacker discovers a weakness, and deploys it first against a SCADA system.

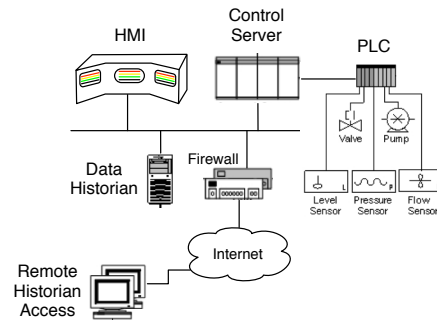
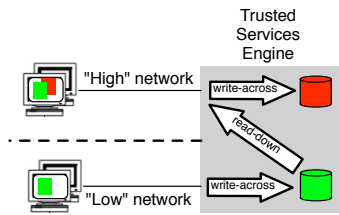


Figure 1: Historian access today

## 3 Opportunity: Re-purposing the Trusted Services Engine

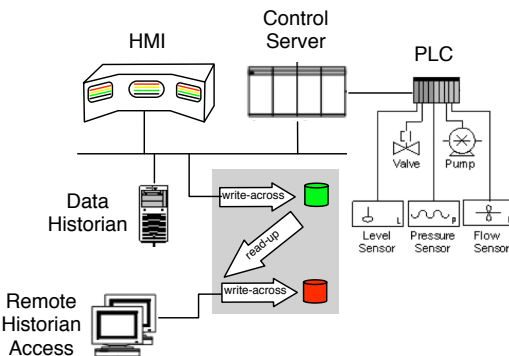
Such circumstances warrant the kinds of security measures, and the “high assurance” methods used to develop them, that are used to protect information on DoD and Intelligence Community (IC) classified “High” networks from leaking to unclassified “Low” networks. Galois has developed the Trusted Services Engine (TSE) [McNamee et al. 2006], a network file store with integrated read-down between security domains, to address cross-domain information sharing, as shown in Figure 2. The methods used to develop the TSE were intended to provide a high level of assurance that data can only flow from lower-classification networks to higher ones, and not from high-to-low. The TSE is designed to prevent data from flowing from high-to-low, and also to ensure that no actions performed by high users or systems (like which file is being read) can be observed in any way at lower networks. This property is called *non-interference*, and provides protection from both direct and covert channels between high and low.

Cross-domain file access is a similar scenario to SCADA Historian security concerns, but with a twist. In a SCADA system the security goal is to isolate the network from any actions (attacks) performed outside the network, while making the Historian data available to



**Figure 2: TSE providing read-down from High- to Low-networks**

those outside networks. We believe that goal could be met with higher assurance than is achieved today by replacing the firewall that allows remote Historian access and replacing it with a TSE. The TSE's "low" network port is attached to the isolated SCADA network, as shown in Figure 3. If the Historian is configured to write its data to the TSE, then outside users on a network attached to the TSE's "high" network are able to "read-up" to the Historian data. The covert channel protection, in this case becomes an isolation argument, that users outside the SCADA network can in no way affect operations inside the SCADA network.



**Figure 3: Historian access through an "upside-down" TSE**

Remote access to Historian data is only one aspect of information assurance challenges in SCADA systems. Building a secure SCADA enclave involves examining and securing *all* network connections. The role of the TSE in the SCADA enclave is twofold: incoming traffic is implicitly denied by the TSE as an inappropriate information flow, while the only outgoing information allowed is in response to requests for Historian data. Other data flows required for the operation of the SCADA system, such as the connection to a remote PLC, would be configured to flow through a separate interface, probably through a Virtual Private Network (VPN), and associated firewall. Further, even though it is not shown in Figure 3, a firewall could be used to guard the Internet-facing port of the TSE in order to filter out some network attacks before they reach the TSE.

#### 4 Comparison to Data Diode

For critical environments, approaches that use a data diode technology (e.g., from Tenix, BAE, Fort Fox or others), are often used to permit historian data to move from a sensitive SCADA control network and less-sensitive networks. Compared to these data diode

approaches, the TSE has a number of advantages:

- *Lower cost* – as a software solution, the TSE will be cheaper to deploy than hardware-based data diodes, which often cost more than \$10,000 apiece,
- *smaller footprint* – since the TSE is software-based, as long as a high-enough assurance operating system platform exists which can provide the needed separation, the TSE components can be hosted for zero footprint on that platform,
- *lower Space Weight and Power* – the SWAP footprint of a TSE-based solution will be lower than a comparable diode based solution, particularly taking into account redundant storage systems at both ends of the diode,
- *higher reliability* – the advantage of a data diode – that data flows in only one direction – makes it a difficult component to build reliable data transfer on top of. It is impossible to request retransmission. The TSE obviates this by storing the data being written by the SCADA historian, effectively buffering it, to be made available at any needed bandwidth by external clients.

The main *disadvantage* of a TSE compared to a data diode is that it has a more complex assurance argument compared to an opto-isolated separation of networks.

#### 5 Next Steps: Identify Sponsors and Partners, Evaluate Approach, Plan Transition

We speculate the following next steps:

- *Identify stakeholders* interested in research towards securing SCADA infrastructure,
- *Identify partners* (possibly groups inside stakeholder organization possibly others) with SCADA expertise, and experimental testbeds suitable for evaluating this proposal,
- *Evaluate the approach* proposed in this white paper,
- If evaluation shows the approach has merit, *plan for transition* towards eventual deployment.

#### References

- CISCO SYSTEMS, INC., 2007. Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances, March. <http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml>.
- KAMARA, S., FAHMY, S., SCHULTZ, E., KERSCHBAUM, F., AND FRANTZEN, M. 2003. Analysis of Vulnerabilities in Internet Firewalls. *Computers and Security* 22, 3, 214–232. <http://www.cs.purdue.edu/homes/fahmy/papers/firewall-analysis.pdf>.
- MCNAMEE, D., HELLER, C., AND HUFF, D. 2006. Building Multilevel Secure Web Services-Based Components for the Global Information Grid. *CrossTalk: The Journal of Defense Software Engineering* (May), 15–19. <http://www.stsc.hill.af.mil/crossTalk/2006/05/0605McNamee-HellerHuff.pdf>.
- STOUFFER, K., FALCO, J., AND SCARFONE, K., 2008. NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security (Final Public Draft), September. [http://csrc.nist.gov/publications/drafts/800-82/draft\\_sp800-82-fpd.pdf](http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf).