

S⁴ SCADA Security Scientific Symposium 2007

January 24 – 25 in Miami Beach, FL

S4 is an event for the presentation of highly technical research papers on SCADA and control system security. Presenters are given one hour to present in detail - - down to the bit, byte, packet, equation, formula, code or script level.

Who should attend: Researchers, engineers and thought leaders in SCADA security.

Who should not attend: Those looking for best practices, standards overviews and case studies. Marketing, sales and managers.

S4 Attendee Options:

Physical Registration: \$995

Join 70 of the best SCADA security researchers and thought leaders in the great Florida weather at [a world class conference facility](#) that is designed for interaction and creative thinking. We have intentionally selected a size and venue that supports an interactive environment.

You will be able to attend all sessions and social activities (including the Vent session) over the two day event, receive a copy of the proceedings, and receive the conference giveaways.

With 15 of the 70 slots designated for speakers and organizers, space is very limited. Register asap to reserve your space.

Virtual Two-Day Attendance, \$600

Travel budgets are tight; SCADA security is a worldwide issue; and physical attendee space is limited.

If you are unable to attend in person, take advantage of our innovative virtual attendee program. A WebEx feed will provide virtual attendees with streaming video window, powerpoint slide window, and a chat/question window for all sessions and keynotes.

SPECIAL: Virtual two-day attendees registering prior to December 1st will receive a copy of the proceedings.

Virtual One-Day Attendance, \$400

Only interested or available for one day? Select the Virtual One-Day Attendance option.

Register online at: <http://www.acteva.com/booking.cfm?bevaaid=120280>

Register Before Dec 31 And Get One Year Subscription To Digital Bond Site

Send questions to S4@digitalbond.com

S⁴ SCADA Security Scientific Symposium 2007

Agenda

Wednesday, January 24th

Keynote: To Be Announced!

Session 1

ICCP Exposed: Analyzing the Attack Surface

Matt Franz, Digital Bond

The Inter Control Center Protocol (ICCP) is actually a complex set of multiple protocols that provides a large attack surface for adversaries and many opportunities for implementers to make errors. In this paper, Mr. Franz explains in detail two of the more interesting layers in the ICCP stack and how attack methodologies commonly seen in other protocols would be applied against the ICCP protocol. Scripts and tools will be used to demonstrate the attacks. Finally, the paper will also discuss what Secure ICCP will and will not do to reduce the attack surface.

Why we selected this paper – ICCP is an important protocol for the reliability of the electric grid. It is one of the few protocols used to share information between different companies. This means holes in firewalls to allow ICCP. The nightmare scenario: one company being compromised and a polymorphic ICCP worm taking down most ICCP servers and any unpatched SCADA servers running Windows.

Session 2

Anonymous, Authenticated Communication for Secure Sharing of SCADA and Control System Information

Timothy Draelos, Annie McIntyre, William Neumann, and Richard Schroepel of Sandia National Laboratories

This paper describes a cryptographic method for an authorized group of users to share digital information with a central collection/analysis/distribution center in an anonymous, yet authenticated way. Sharing of information within the SCADA and process control community is important for understanding threats and early detection of coordinated attacks. Sharing sensitive information attributable to a particular user has risks that our technological solution can mitigate. The receiving center can ensure that an arriving message is from a member of the group, but cannot (nor can electronic eavesdroppers) determine which member of the group sent the message. This method involves an ordinary public key infrastructure and hardware tokens for distribution of key material. Since anonymous communication opens the door for untraceable system abuse, our solution employs a multi-level communication structure that mitigates abuse by allowing message revocation, yet retains true anonymity at the highest level. Anonymous, authenticated communication is an enabling technology to secure sharing of SCADA and process control system information.

S⁴ SCADA Security Scientific Symposium 2007

Why we selected this paper – SCADA and other critical infrastructure information sharing efforts have failed to date because asset owners have not participated in sufficient numbers. One reason for low participation is the fear that sharing attack and incident information could harm an organizations reputation. After all, how many times have you heard about the Australian wastewater hack? Perhaps anonymous information sharing will increase participation, but it is a difficult technical problem.

Session 3

A Methodology for Estimating the Mean Time-to-Compromise of a System

Eric Byres, Byres Security

David Leversage, British Columbia Institute of Technology

The ability to efficiently compare differing security solutions for effectiveness is often considered lacking from a management perspective. To address this we propose a methodology for estimating the mean-time-to-compromise (MTTC) of a target device or network as a comparative metric. A topological map of the target system is divided into attack zones, allowing each zone to be described with its own state-space model (SSM). We then employ a SSM based on models used in the biological sciences to predict animal behavior in the context of predator prey relationships. Markov chains identify predominant attacker strategies which are used to build the MTTC intervals and can be compared for a broad range of mitigating actions. This allows security architects and managers to intelligently select the most effective solution, based on the lowest cost/MTTC ratio that still exceeds a benchmark level.

Why we selected this paper – First, it wouldn't be a SCADA research conference without Eric. Second, calculating risk and making the business case for SCADA security is a huge issue for the industry. This paper's mathematical approach is a very interesting contribution to the topic, and the parameters provide some guidance on the most effective way to increase the mean time to compromise.

Session 4

Using Model-based Intrusion Detection for SCADA Networks

Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Sinner and Alfonso Valdes, SRI International Computer Sciences Laboratory

Control systems tend to have static topology, regular traffic and a limited number of simple protocols. Monitoring of control systems for security is therefore potentially easier than in enterprise systems. In particular, we hypothesize that model-based monitoring, which offer the promise of detecting zero day attacks, may be more feasible in control systems. In the model-based approach, we construct models that characterize the expected/acceptable behavior of the system, and detect attacks that cause the system to behave outside of the models. In this paper, we explore this hypothesis and describe the implementation of a lightweight model-based monitor in a control system testbed.

S⁴ SCADA Security Scientific Symposium 2007

Why we selected this paper – Signature based IDS is effective but limited to detecting known attacks. Anomaly detection for IDS/IPS is a promising technology that could identify zero-day attacks and system misuse that would be missed by a signature based system. Control systems would seem to be an ideal environment for detecting anomalies.

Session 5

Crypto Algorithm Performance on Common Field Device Processors

Bill Lattin, Certicom

PLC's, RTU's and IED's have stringent performance requirements but often have CPU's on the controller and interface cards with limited processing power. This paper will answer the question of what is the impact of digital signature, encryption, secure hash and other crypto primitives on CPU's and memory found in leading field devices. The performance implications of different algorithms such as RSA, elliptic curve and Diffie Hellman will be explained.

Why we selected this paper – The community has assumed current processors can't run crypto algorithms. Let's prove or disprove this theory. Additionally, the community needs to start looking at what protocols are the most efficient for securing field communications.

Session 6

SCADA Protocol Obfuscation: A Proactive Defense in SCADA Systems

Carlo Bellettini and Julian L. Rrushi, Dipartimento di Informatica e Comunicazione, Università degli Studi di Milano

This paper describes a defensive approach and demonstrates that approach using MODBUS-TCP. We build our defensive approach upon information reflected in what we call an attack requirements tree. We then show how an obfuscation of a SCADA protocol can neutralized fundamental elements necessary for carrying out a SCADA protocol-based attack. The paper describes an obfuscation algorithm and code obfuscation techniques to hide the fundamental organization of such an algorithm. An estimate of the computational and networking overhead induced by this defensive approach is included as are potential attack scenarios on this approach.

Why we selected this paper – It is a very different approach. There is such a focus on minimizing overhead, and this approach specifically adds overhead to make it difficult for an attacker to identify meaningful requests and response data. Some times communities get stuck in a rut, and it requires a counterintuitive idea to break out of that rut. We are not proclaiming this is it, but let's have some leading researchers in the audience consider a different path. It may spawn some new ideas.

S⁴ SCADA Security Scientific Symposium 2007

Thursday, January 25th

Session 7a

OPC Exposed: Denial of Service Attacks

Ralph Langner, Langner Communications AG

It is well known that OPC does not include effective security controls and relies on DCOM. Well, the problem is much larger than that. In this paper, several DoS attacks that have proven effective against OPC servers are discussed that could be carried out by attackers with no technical background or by malware. In addition, a man-in-the-middle attack is explained that could be used by an aggressive attacker to have a SCADA system assume normal operation while the process is running wild. Last but not least, suggestions for remedies are presented.

Session 7b

OPC Exposed: Protocol Analysis and Security Testing

Lluís Mora, Neutralbit

Although MSRPC services have been widely tested for security vulnerabilities, the tests have centered around the transport layer and not on the application layer that DCOM implements. In this paper, we present a security analysis of the Data Access specification with emphasis on the application layer, identifying theoretical weaknesses that implementers should take into consideration when developing OPC clients and servers. To validate our findings a vulnerability group test has been conducted against several OPC servers.

Why we selected these papers – Sessions 7a and 7b are parallel presentations to ICCP Exposed; OPC is another protocol that is frequently used to exchange information outside of the control center. Too often analysis is restricted to “there is no security in OPC” or “it uses DCOM”. These two papers provide detail from two different approaches. Ralph focuses on the robustness, or lack thereof, to resource exhaustion and other denial of service attacks. We knew this paper had to be included when we saw Ralph’s OPC Doom tool. Lluís from Neutralbit looks at the protocol itself and identifies areas where buffer overflows and other application layer attacks may be effective in poorly coded applications. Lluís has a tool as well that we are anxious to get our hands on. Note both of these presentations come from Europe, Germany and Spain.

Session 8

Identifying Attacks on Control Systems by Scripting Event Aggregation and Correlation

Ron Gula, Tenable Network Security, Inc.

Statistical event models can aggregate data from multiple sources and correlate security events to detect attacks on SCADA and other control systems. Most Security Event Management (SEM) solutions have this capability, but it requires an understanding of the system and scripting to build in the SCADA intelligence. In this paper we will discuss how to build aggregation and correlation rules using the scripting languages. SCADA events will be used as examples and TASL scripts will be provided.

S⁴ SCADA Security Scientific Symposium 2007

Why we selected this paper – Three reasons 1) Detection is an important component of any security program. In SCADA it is crucial because most SCADA systems and protocols lack appropriate protection. 2) We are a big believer in adding SCADA intelligence to existing security solutions 3) Ron has an impressive track record with Dragon and Nessus and is usually at the forefront of some new interesting security approach.

Session 9

Automated Testing of SCADA Protocols

Nate Kube, Wurldtech Security

Testing is an important part of the Quality Assurance (QA) process, and the security portion of QA can detect potential vulnerabilities prior to exploitation. This paper begins by presenting background information on protocol testing and the available tools. We then discuss our experience in developing blackPeer, the testing framework for SCADA protocols in Achilles, including lessons learned and key design decisions. The paper includes detail on the employment of blackPeer in conformance testing of SCADA devices and summarizes the errors found. We conclude with observations on how the SCADA community can better ensure the security of its control systems.

Why we selected this paper – This is the engine in the Achilles platform that we have been hearing about for years. We were interested in how the engine was built, the evolution of the design decisions as results from SCADA devices came in, and the common results found from the testing that would indicate areas where SCADA device coding needs to be improved.

Session 10

N-Secrecy Authentication Response to Graduated Threat Levels in SCADA Networks

James H. Graham and Waleed Elsaid of the Intelligent Systems Research Laboratory at the University of Louisville

Authentication of the communications between the master terminal units (MTU's) and the remote terminal units (RTU's) is one of several enhancements needed to improve SCADA system security. This paper presents a new approach to communications security, which we term N-secrecy authentication, which implements a multiple-level, light-weight authentication service, based upon symmetric encryption and N-shared secrets between an MTU and an RTU. This authentication architecture facilitates increasing security as the system threat level increases. Threat level can be assessed in a variety of ways, including a computationally efficient approach using fuzzy logic inference. Preliminary evaluation of the fuzzy logic threat-level assessment and the N-secrecy authentication algorithm indicates significantly enhanced SCADA system security at reasonable overhead levels.

Why we selected this paper – Authentication of the source and data in SCADA communication is typically the most important SCADA security requirement, as opposed to encryption for

S⁴ SCADA Security Scientific Symposium 2007

privacy. The community needs to start developing and vetting SCADA authentication security protocols with the goal of standardizing on a small number of security protocols.

Session 11

SCADA Honeynets in Two Parts

Part 1: How to Build SCADA Honeynets

Part 2: Analyzing Attacks on SCADA Honeynets

Landon Lewis, Digital Bond

Part 1 of this paper describes the design of a SCADA Honeynet that appears to be a PLC running Modbus TCP and management interfaces, the factors that make the SCADA Honeynet realistic and high interaction, and different scenarios for exposing SCADA Honeynets. Part 2 of the paper is a statistical analysis of attacks on the SCADA honeynet and a detailed analysis of the more interesting attacks at the packet level.

Why we selected this paper – SCADA Honeynets provide a rare opportunity for the community to review detailed attack information on SCADA devices. What do attackers do when they encounter a PLC? A secondary reason for selecting this paper is a hope that greater understanding of this technology will lead to the development of enhanced SCADA Honeynets and increased deployments.

<<Conference and Hotel Logistics are on the following pages>>

S⁴ SCADA Security Scientific Symposium 2007

Conference Location:

The Conference will be held at the Florida International University (FIU) Kovens Conference Center. This is a beautiful facility, and ideally suited for interaction between 70 top SCADA security researchers. The sessions will be held in a small auditorium, case study room designed for interaction.

Lunch will be served outside, on the terrace overlooking the intercoastal waterway in the beautiful January Florida weather.

Transportation will be provided from the conference hotel to the Kovens Center.



Session Room



Terrace Overlooking The Intercoastal

There is plenty of free parking at the Kovens Conference Center and transportation from the Conference Hotel and the Conference Center will be provided. The Kovens Conference Center is located on the Biscayne Bay Campus of Florida International University. The entrance is at NE 151st Street and Biscayne Blvd. in North Miami. Take NE 151st Street approximately 1.5 miles, following the signs to the Roz & Cal Kovens Conference Center.

[Directions and map to the Kovens Conference Center.](#)

S⁴ SCADA Security Scientific Symposium 2007

Conference Hotel

The [Doubletree Ocean Point Resort & Spa on Miami Beach](#) is the official conference hotel. It is right on the beach, and a short ride from the FIU conference center. It is also a short ride from the infamous South Beach scene.



A limited number of rooms are available at the S4 rate of \$195. Reserve your room online at: http://www.hilton.com/en/dt/groups/personalized/miaopdt_dig/index.jhtml.

There are additional hotels nearby:

- The Trump (Sunny Isles)
- Courtyard By Marriott Aventura
- Hampton Inn (Hallandale)