



SCADA Security Scientific Symposium 2008

January 23 – 24 in Miami Beach, FL

S4 is a unique 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 senior management.

S4 Attendee Options:

Physical Registration: \$995

Join 60 of the best SCADA security researchers and thought leaders in the great Florida weather at a world class conference facility, <http://www.kovens.fiu.edu/> 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 over the two day event, receive a copy of the S4 Proceedings book, and receive conference giveaways. Additionally this year we will make a significant portion of the Digital Bond lab available for you to pound away on to experience the joys of testing control systems with your favority bag of tools.

With 15 of the 60 slots designated for speakers and organizers, space is very limited. Register asap to reserve your space.

Virtual Two-Day Attendance, \$800

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 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. Virtual attendees loved the experience last year, although the virtual attendees in Asia and Australia were sleep deprived. Two-day virtual attendees will also receive a copy of the S4 Proceedings Book.

Virtual One-Day Attendance, \$600

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

Register online at: <http://www.acteva.com/booking.cfm?bevalID=144585>

Register Before Dec 23 And Get A One Year Subscription To Digital Bond Site (a \$100 value)



SCADA Security Scientific Symposium 2008

Agenda

Wednesday, January 23rd

Day 1 Keynote: Steve Lipner of Microsoft

Lessons Learned While Building Secure Software

Steve is responsible for the definition and updating of the Security Development Lifecycle Process that Microsoft applies to improve the security and privacy of their products. He is also a co-author with Michael Howard of the book, *The Security Development Lifecycle*. All physical attendees will receive a copy of this book.

The control system vendor community is where Microsoft was back in 2002, or worse. It just has not been subjected to the massive amount of scrutiny that Windows and other Microsoft products have. It is time for control system vendors to improve the software security, and who better than Steve to provide some ideas and hard data on what is working at Microsoft.

Session 1

Security Assurance Levels: A SIL Approach to Security

Nate Kube of Wurdtech Security Technologies

A Safety Integrity Level (SIL) is a statistical representation of the reliability of the Safety Instrumented System (SIS) when a process demand occurs. SIL's are correlated to the probability of failure of demand (PFD), which is equivalent to the unavailability of a system at the time of a process demand. Given that the exploitation of security vulnerabilities can result in a system becoming unavailable, this paper proposes the concept of Security Assurance Levels (SALs) and demonstrates how one such level could be constructed with pass/fail criteria, measurement, device monitoring and a test bench. The paper concludes with a vulnerability taxonomy that results from the cross product of the monitor states.

Why we selected this paper – We have heard so often the security comparison to safety and the desire to have the security equivalent of Safety Integrity Levels (SIL's). This is the first paper we have seen that attempts to create this equivalent with a measurable and testable Security Assurance Level (SAL).

Session 2

Threat Modeling of NetDDE Vulnerabilities as used in Control Systems

Xavier Panadero of Neutralbit and Edmundo Farinas of Digital Bond

The NetDDE protocol facilitates communication between DDE-aware applications, including SCADA applications. In this paper we will identify vulnerabilities in the NetDDE



SCADA Security Scientific Symposium 2008

implementation and configuration and create a threat model for a selection of these vulnerabilities. One of the vulnerabilities will be discussed in depth and demonstrated with an attack on a popular HMI that allows an attacker to remotely execute arbitrary commands on the HMI.

Why we selected this paper – Xavi and the Neutralbit team followed their great work on OPC from last year with this analysis of NetDDE used by popular HMI's. Digital Bond is pleased to assist in applying threat modeling to their work and co-writing the paper. The disclosure issues related to the vulnerability will be completed by S4 as there already is a security patch available.

Session 3

Measurable Control System Security through Ideal-Driven Technical Metrics

Sean McBride, Miles McQueen, Wayne Boyer, and Robert Nitschke of Idaho National Labs (INL); Marie Farrar and Zach Tudor of Securicon

The Department of Homeland Security National Cyber Security Division developed a small set of security Ideals as a framework to establish measurable control systems security. Based on these Ideals, a draft set of proposed technical metrics was developed to allow control systems owner-operators to track improvements or degradations in their individual control systems security posture. This paper discusses several weaknesses found in previously defined technical metrics, defines the seven Ideals used to guide the metrics development, presents the initial proposed set of technical metrics, and performs an initial validation of the metrics using the general findings and recommended mitigations from previous control system security assessments. Gaps between the assessment findings and the proposed ideals and metrics are identified and improvements are suggested.

Why we selected this paper – Eric Byres paper last year on Mean Time to Compromise and subsequent discussions on the importance of measuring risk and risk reduction show this is an area of great interest to the community. An accepted methodology to quantify the risk or security level is critical to providing C-level executives the information required to allocate money and other resources to control system security.

Session 4

Modeling Flow Information and Other Control System Behavior to Detect Anomalies

Brian Moran and Richard Belisle of IBM / Internet Security Systems

The stereotypical behavior of most control systems lends itself to modeling the system and detecting anomalies that could be used to detect possible cyber attacks, or other dangerous network activity in real time. In this paper we will discuss and demonstrate how the flow information available from routers and other network devices can be used in an anomaly detection system (ADS) to detect attacks from the normal communication flows from a source / destination / service perspective, without impacting the real-time processing requirements of the control system. The paper will discuss in detail how an ADS systems can be used to model control system protocol usage to detect anomalies caused by cyber attacks, or other malicious



SCADA Security Scientific Symposium 2008

behavior that is becoming more pervasive in control system environments. Finally, the paper will discuss the research going into next generation ADS systems and how they will be even more useful in modeling control system environments.

Why we selected this paper – The first sentence says it all - - “stereotypical behavior of most control system lends itself to modeling the system and detecting anomalies”. We believe anomaly detection in control systems holds great promise, and we chased papers on this subject. This paper had the added benefit of leveraging readily available flow information from routers.

Session 5

Detecting Attacks in Power Plant Interfacing Substations through Probabilistic Validation of Attack-Effect Bindings

Julian L. Rrushi and Roy H. Campbell, University of Illinois, Champaign-Urbana

This paper proposes a mathematical technique for detecting attacks on IED’s implementing the IEC-61850 protocol within an electric substation. The technique uses two different models: a flow model based on stochastic activity networks and a probabilistic attack model. These two models are joined to create a composed probabilistic model which is used to emphasize bindings between potentially offensive protocol frames and their corresponding impact on IEC-61850 functional and data resources. Attack-effect bindings get further characterized through their temporal, causal, and spatial relationships. The paper describes experimentation with a SEL-4000 adaptive multi-source channel device simulating electric power flow, a network of SEL-421 relays speaking IEC-61850 and simulating a substation, and an OSI OSIRIS RTU speaking Modbus and providing status and control data.

Why we selected this paper – The focus on IEC-61850 and the use of equipment commonly found in substations make this paper unique. Additionally, the effort to combine a flow model with an attack model is interesting. The increased data from different perspectives potentially could lead to better detection decisions.

Session 6

Wireless Security in DCS

Why we selected this paper – Actually we have not received or found a quality paper on wireless, but we are committed to finding some great work.

Cocktail Reception Overlooking The Intercoastal Waterway



SCADA Security Scientific Symposium 2008

Thursday, January 24th

Day 2 Keynote: Dave Aitel: The Hacker Strategy

How would a highly skilled and highly motivated hacker attack an application and system they had never seen before? Perhaps a critical infrastructure control system that some entity is willing to pay to have taken down or have access to or even remotely control. Dave Aitel will answer this question.

Dave Aitel has worked at the US National Security Agency, the consulting firm @stake (now Symantec), and is the founder and CTO of Immunity, Inc. He is known for groundbreaking vulnerability research as the author of the first block-based protocol tester, SPIKE. Mr. Aitel is the co-author on The Shellcoder's Handbook which is the go-to book for learning how to write exploits and buffer overflows. As CTO of Immunity, Mr. Aitel has helped launch the first Vulnerability Sharing Club, an exploit-focused debugger, a visual language for writing buffer overflows, SILICA, a hacking tool that fits in your pocket, and Immunity's flagship product, a penetration testing toolkit, CANVAS.

Session 7

Control System Attack Vectors and Examples: Field Site and Corporate Network

Eyal Udassin, C4

Attacking a SCADA or DCS from the control center is difficult due to the physical security and 24 x 7 operations. In this paper we discuss attacks from two more accessible locations with logical access to the control center: field sites and the corporate network. The attack vectors will be profiled and then specific examples will be provided and demonstrated with widely used systems. A heap overflow from a field site will be described that both crashes a control server and provides elevated privileges. A successful attack from the corporate network will provide remote control of a reporting server using only protocols that are allowed through a well configured firewall.

Why we selected this paper – We significantly altered this abstract to avoid pre-patch disclosure issues that will be resolved by S4, but we predict this paper will really open some eyes. The attack vector theory is interesting and the compelling results and demonstrations on popular control system software will address FUD-sayers out there. These are attacks that would be successful even in a best practice perimeter security configuration.



SCADA Security Scientific Symposium 2008

Session 8

Risk Awareness through Cybersecurity Attack Scenarios

Ralph Langner of Langner Communications and Bryan Singer of FluidIQs

Risk is commonly defined as threat x vulnerability x damage. While a simple equation, in real life this is almost impossible to fully quantify, especially those that are imposed by malicious attackers. This paper offers an alternative by taking a step back from the risk equation to posit the "what if." This approach defines the roots of risk by using scenarios to help illustrate the potential impacts to operations, centering around determining attacker clusters in respect to motivation and intent. Successful criminal acts are usually analyzed in terms of three items: Motive, Opportunity, and Means (MOM). As such, this paper works from the mind of the attacker and takes into account these factors to determine what are some likely possibilities for cybersecurity events.

Why we selected this paper – This was a tough call because we questioned if this paper would have enough technical meat for S4. We were won over by the strength of the authors, the early work that each author had done independently, and the fact that this is a compelling topic. We have no doubt this topic will generate a lot of discussions and an effort to formalize this type of analysis is worthwhile.

Session 9

Key Management and Cryptography for Advanced Metering Infrastructures (AMI) and Other Large, Low Power Networks

Grant Gilchrist, EnerNex

Advanced Metering Infrastructures (AMI) have limitations that require unique information security approaches. Some of the characteristics addressed in this paper include the mixture of one-way broadcast and two-way communication, the limited processing power found in an organizational issues in managing cryptographic credentials, the sheer number of endpoints (in the millions) and the expected type and frequency of message traffic to be addressed. This paper describes an authentication mechanism for the broadcast network and discusses alternatives under consideration for securing the two-way AMI networks including securing a variety of wireless protocols used in these networks.

Why we selected this paper – This AMI application represents an extreme example of the SCADA environment with a one-to-many, low bandwidth, low processing power and low cost required in the security software and hardware. AMI is a bit unique in that security compromises can be directly tied to lost revenue from billing fraud. If a key management protocol can be made to work in this environment it should work in most SCADA environments.



SCADA Security Scientific Symposium 2008

Session 10

Maintaining PCS Functionality Despite an Active Cyber Exploitation

Ron Pawlowski, Pacific Northwest National Laboratory (PNL)

Identifying cyber attacks is an important first step, but the real goal is to prevent attacks from affecting control system performance. In this paper techniques to mitigate the consequences of a cyber vulnerability exploitation will be proposed and assessed. File monitors can watch for unauthorized changes in critical data stores. Process monitors can keep critical processes running, and can terminate unauthorized processes. Checkpoint and restore schemes can recover a system to its last known healthy state. These systems show promise for general-purpose computing applications. However, PCS computers have additional requirements related to timing and communications - often they must operate in real-time. Can these protection schemes be used to help PCS computers ride through, fight, and perhaps defeat an on-going cyber attack? The paper will discuss the implementation and testing experience of the more promising technical approaches in PNL's Security Hardened Attack Resistant Platform (SHARP).

Why we selected this paper – We all know availability is the primary control system concern in the C-I-A security triangle. This is typically provided through careful selection of hardware and redundancy, which is not particularly effective against directed cyber attacks. This paper describes methods to maintain availability under an active attack which is novel.

Session 11

OPC UA Exposed

Dale Peterson, Digital Bond

The recently published OPC Unified Architecture (UA) protocol was developed with integrated security features, which is unique for a control system protocol. In this paper we will detail the protocol's security measures and discuss the strengths, weaknesses and open questions of the security in OPC UA. Additionally, the paper will analyze the OPC UA attack surface and implementations provided by the OPC Foundation. Given that OPC UA defines XML and UA Binary for data encoding and TCP and SOAP web services for transport.

Why we selected this paper – Well . . . it is our own contribution to the event. OPC UA is an ambitious set of standards with significant claims of security. This is the time to shake it out and identify vulnerabilities before it is deployed.

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



SCADA Security Scientific Symposium 2008

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

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. There is plenty of free parking at the Kovens Conference Center.



SCADA Security Scientific Symposium 2008

Conference Hotel

The Doubletree Ocean Point Resort & Spa on Miami Beach, 1-786-528-2500 / <http://doubletree.hilton.com/en/dt/hotels/index.jhtml?moreDesc=true&ctyhocn=MIAOPDT>, 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.

Reserve your room at the Conference Hotel:

<http://doubletree.hilton.com/en/dt/groups/personalized/MIAOPDT-S4D-20080119/index.jhtml>

Want to arrive early or stay the weekend in South Beach? Take advantage of the great conference rate at the Doubletree.



A limited number of rooms are available at the S4 rate of \$199. This is a great price for a hotel right on the beach in season. Reserve your room online at:

There are additional hotels nearby:

- The Trump (Sunny Isles)
- Courtyard By Marriott (Aventura)
- Hampton Inn (Hallandale)
- Le Meridien (Sunny Isles) (The nicest property on the ocean in the area)

Sponsor Opportunities

S4 offers a unique virtual attendee program that provides a live Internet feed of the video and presentations to a worldwide audience. Virtual attendees are able to participate in an online chat with other virtual attendees and participate in the Q&A. Virtual attendees were thrilled with the experience in S4 2007.



SCADA Security Scientific Symposium 2008

To support the virtual attendee program and raise your corporate profile to physical and virtual attendees Digital Bond is offering one, and only one, sponsorship for each day of S4.

- Sponsor PowerPoint slide or slides presented in physical room and to virtual audience during all breaks
- Sponsored by “skin” for Virtual Attendees throughout the event
- Sponsor sign in the physical room throughout the day
- Sponsor thank you and acknowledgement at the beginning of the morning and afternoon session
- Sponsor banner and links on Digital Bond’s website through the S4 Event. Digital Bond’s website is the most popular and widely viewed control system security resource on the Internet.