

DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



## S4 ON JAN 18 – 19 IN MIAMI BEACH ADVANCED TRAINING ON JAN 17 AND 20

S4 is a unique event for the presentation of highly technical research on SCADA and control system security. Now in its 5<sup>th</sup> year, S4 was created because there was and is no other venue to present this type of work. The audience is filled with technical experts and thought leaders in this space so there is no wasted time discussing the basics of ICS and security. Sessions have significant technical detail - - down to the bit, byte, packet, control, protocol, statistic, code, or script level. The S4 audience represents the best minds in control system security research and a highlight of the event is the discussions and relationships you will develop.

**Who should attend?** Researchers, engineers & thought leaders in ICS security.

**Who should not attend?** Those looking for best practices, standards overviews and SCADAsec 101. Marketing, sales and those with a non-technical background.

The 2012 edition has more content and the strongest agenda to date. To squeeze all this good work in we have introduced 30-minute and 45-minute sessions, in addition to the traditional one-hour session. The result is a lot more leading edge content.

The advanced training prior in conjunction with S4 is quite popular with students not having to sit through what is SCADA, C – I – A, and other 101 level topics. In 2012 we have *Hacking and Exploiting HMI and EWS* on the day prior to S4 and *Hacking and Exploiting PLC's* the day after S4. Consider extending your time in Miami Beach to four days or longer.

### PRICE

S4 is limited to 60 attendees, including the speakers, because it is held in a case study room specifically designed for participation and interaction. Don't miss your chance to attend.

S4 Conference (two days):	\$995
S4 Conference + 1 Advanced Training (3 days):	\$1,645
S4 Conference + 2 Advanced Training (4 days):	\$2,145

[Click Here To Register](#)



DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



## S4 2012 AGENDA AT A GLANCE

### JAN 17, PRE-EVENT TRAINING

9:00 – 4:00            Hacking and Exploiting HMI and EWS

### JAN 18, DAY 1:

8:30 – 9:15            Keynote – To Be Announced

9:15 – 10:00          The Witch Doctor vs. the Engineer – Why Believe Either One?

10:00 – 10:30        Technical Security in Smart Metering Devices: A German Perspective

10:30 – 10:45        Break

10:45 – 11:30        Documenting the “Lost Decade:” An Analysis of Publicly-Disclosed ICS-Specific Vulnerabilities since 2001

11:30 – 12:15        Forensic Evidence and Investigation in Stuxnet

12:15 – 1:15          Lunch on the patio overlooking the intercoastal waterway

1:15 – 1:30            Unsolicited Response

1:30 – 2:00            Automated Consequence-Based Assessment Schema

2:00 – 2:45            Social Engineering Industrial Control Systems

2:45 – 3:00            Break

3:00 – 4:15            Application Whitelisting in ICS (2 Presentations)

                              Part 1 – Application Whitelisting for Industrial Control Systems - An Evaluation Guideline

                              Part 2 – No Silver Bullets: Application Whitelisting in ICS

4:15 – 4:30            Faking Out Security Enumeration Tools

4:30 – 5:15            Correlating Process Events with Security Events to Detect Attacks

5:15 – 7:30            5<sup>th</sup> Annual S4 Cocktail Party



DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



## JAN 19, DAY 2:

8:30 – 10:30	Project Basecamp: Hacking and Exploiting PLC's Part I: PLC Attack Methodologies and Analysis of Overall Results Part II: Specific PLC Attacks and Exploit Examples
10:30 – 10:45	Break
10:45 – 11:15	Denial of Surface?
11:15 – 12:00	Preventing Attacks on Critical Infrastructure through Hardware Protection Against Malicious USB Devices
12:00 – 1:00	Lunch on the patio overlooking the intercoastal waterway
1:00 – 1:15	Unsolicited Response
1:15 – 1:45	Intrusion Detection for Embedded Control Systems
1:45 – 2:00	Lessons Learned From Certifying Embedded Devices
2:00 – 3:00	The Great Debate: Anti-virus and Monthly Security Patching Should Be Abandoned in ICS
3:00 – 3:15	Break
3:15 – 4:00	Live Forensics in Control Systems
4:00 – 4:30	To Be Announced
4:30 – 4:45	Closing Remarks

## JAN 20, POST-EVENT TRAINING

9:00 – 4:00	Hacking and Exploiting PLC's
-------------	------------------------------





## S4 ADVANCED TRAINING JANUARY 17 AND 20

Digital Bond is offering two advanced training courses in conjunction with S4, one before and one after the main S4 conference. These are advanced courses so students are expected to know what a control system is and the basics of networking and information security.

Registration for the courses must be in conjunction with S4 registration. One course will be an additional \$650 and two courses will add \$1,150 to the S4 registration fee. Each course begins at 9AM and is done by 4PM. Transportation to and from the conference hotel will be provided.

The courses are being developed in Q4 2011, so they will have the latest and greatest info and examples. Each course will be approximately 1/3 lecture and 2/3 lab.

### JAN 17<sup>TH</sup>: HACKING AND EXPLOITING HMI AND EWS

HMI and EWS have comprised most of the vulnerabilities to date, largely because they are an easy component for researchers and hackers to obtain. In this class you will learn attack methodologies that have been successful in compromising HMI/EWS. The theory of the attacks will be described in lectured, demonstrated, and then performed by the students on actual ICS HMI and EWS.

For students who finish the labs quickly, the course will have HMI that have not yet been exploited available for testing using the theory and tools taught in the class.

An equally important part of HMI/EWS hacking is how to leverage a successful attack on an HMI to pivot and attack the process itself. You control the HMI ... now what are you going to do with it. The course will have different process attack paths described in lecture and then a subset of these implemented by students in labs.

### JAN 20<sup>TH</sup>: HACKING AND EXPLOITING PLC'S

This course will be based largely from the work on Project Basecamp where six researchers have attempted to exploit PLC's in at least eight different attack categories. The course will have the PLC's used in Basecamp as part of the lab portion of the course, and these PLC's are popular, widely used devices in critical infrastructure ICS.

In this course you will learn attack methodology that was found to be successful against PLC's and have hands on experience with some of the more effective tools that identify the vulnerabilities. A small number of the vulnerabilities will have corresponding exploit labs.

Finally, the course will lay out a taxonomy of PLC-based attacks, that is what an attacker would do with various types of PLC exploits. Examples will be demonstrated and extra credit labs will be available for advanced students.





## S4 2012 DETAILED AGENDA

### DAY 1:

8:30 – 9:15                      Keynote: To Be Announced

Expect a surprise in the S4 Keynote. It is never a common ICS security type. S4 keynotes are selected from leaders in related fields to provide a new perspective to the ICS security challenge. Past keynoters include Whit Diffie on creating a security community, Steve Lipner on developing secure code, Ross Anderson on the economics of security, Dave Aitel on elite and targeted hacking, and Kris Harms from Mandiant on APT. All S4 keynotes introduced new topics to the ICS security community that subsequently became mainstream issues and presentations. The S4 keynote will help you stay on the leading edge.

9:15 – 10:00                      The Witch Doctor vs. the Engineer – Why Believe Either One?  
Darren Highfill, Utilisec  
James Ivers, Len Bass, and Howard Lipson, Software Engineering  
Institute at Carnegie Mellon; Jim Nutaro, Teja Kuruganti, and Glenn  
Allgood, Oak Ridge National Lab

It's called "security engineering," but in truth most modern security efforts are characterized by substantial use of tribal knowledge and arbitrary checklists that are used often enough to be called "best practices." Non-security business types view security as a black art – opaque to outside understanding – and rely heavily on their security experts to give them the nod that enough security has been baked in.

This paper will take an unflinching look at the state of our industry and how security recommendations and requirements are developed today. We will break down the modern approach and demonstrate how even wide review by a spectrum of "experts" should not be acceptable for any of us, and continues to perpetuate the cycle of discover-and-patch. We will then proceed to propose an approach used by the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) that we believe has the potential to eventually provide "provable" security. We will discuss the known shortcomings of the ASAP-SG approach, how these shortcomings might be addressed, what work remains to be done, and where we still have questions. Finally, the paper will ask if the ASAP-SG approach is a



tangible step forward, or if we are really just better off offering up chicken bones for the witch doctor.

10:00 – 10:30      Technical Security in Smart Metering Devices: A German Perspective  
Stephan Beirer and Holm Dening, GAI NetConsult

In a smart grid environment, smart meters are the most exposed part of the infrastructure. Nevertheless it is a crucial link in the chain of security for advanced smart grid functions. With this in mind, German utilities began to develop a Common Criteria Protection Profile (PP) for the communication gateway of smart metering systems which was adopted and advanced by the German Federal Office of Information Security. According to current German legislation a successful evaluation a new smart metering device is mandatory before it is approved for the use in household installations.

This presentation will introduce the key elements of the PP for smart metering gateways. The threat model, security objectives and the defined security functions, in particular for switching and local load shedding, will be specifically discussed. For a better understanding of specific security requirements this talk will also clarify the elevated importance of privacy issues in Germany and the corresponding security features defined in the PP.

The talk will conclude with an outlook at the current stage of design specifications for the communication protocols between smart metering components in accordance with the PP.

10:30 – 10:45      Break

10:45 – 11:30      Documenting the “Lost Decade:” An Analysis of Publicly-Disclosed  
ICS-Specific Vulnerabilities since 2001  
Sean McBride, Critical Intelligence

In mid-2010, SCADA and Industrial Control Systems (ICS) security officially “came of age” with the first documented malware specifically leveraging a publicly-known vulnerability in ICS. The Stuxnet worm and the subsequent Beresford vulnerabilities were hailed as a turning point for information warfare and nation-state capabilities, a harbinger of things to come. This paper and presentation will:

- 1) Present a detailed statistical analysis of the 250 public ICS-specific vulnerabilities disclosed over what some thought leaders have termed “the lost decade.”
- 2) Compare ICS-security timelines with external “non-ICS” security events
- 3) Empirically examine the efforts expended to discover, disclose, and mitigate ICS-specific vulnerabilities



- 4) Provide a set of recommendations for vendors based on the foregoing statistical analysis, timeline correlation, and empirical observations.

11:30 – 12:15      Forensic Evidence and Investigation Details in Stuxnet  
Ralph Langner, Langner Communications

There have been a large number of Stuxnet talks, but this presentation can only take place at S4 where the audience has a deep understanding of ICS and infosec. Ralph will go deep into a level of details not yet seen. Here is just one example: Ralph will explain how one can see the IR-1 cascade within pseudo-code derived from Stuxnet's STL code.

12:00 – 1:00      Lunch on the patio overlooking the intercoastal waterway

1:00 – 1:15      Unsolicited Response

Three S4 attendees are given five minutes each to talk about an ICS security research project, rant about an issue that is bothering them, respond to an earlier presentation or bring up any topic they like. The Unsolicited Response can be a rehearsed presentation or off the cuff, impromptu stream of consciousness.

1:30 – 2:00      Automated Consequence-Based Assessment Schema (CBAS)  
Dennis Holstein, OPUS Consulting Group

Given the complexity of the threat landscape coupled with the functional complexity of control systems it became clear that a highly-automated, consequence-based assessment schema was needed to adequately assess the consequences and impact of a cyber attack on these systems. A control system CBAS taxonomy with an embedded UML model will be described along with pertinent examples, such as its use in ESCoRTS and CIGRE.

The author contends CBAS provides a major advance over other assessment technologies to analyze threat agents, targets, vulnerabilities and consequences. CBAS includes additional analytic capabilities, including collaboration among actors, simultaneous consequences and time dependence of consequence.



2:00 – 2:45                      Social Engineering Industrial Control Systems  
Anonymous (no not that Anonymous)

Most critical infrastructure ICS that care about cyber security are segmented from the corporate network with an ICS firewall often with one or more DMZ to mediate required communication. Even in these more secure environments it is common for a small number of systems belonging to key applications or administrators to be allowed through the firewall to the ICS.

In this presentation two researchers are, with appropriate approvals, performing a social engineering attack in an attempt to gain control of a system or user credentials on the corporate network that is allowed through to the ICS. The Social Engineering Toolkit (SET) is being used, but the social engineering attacks are using ICS specific information and knowledge to lure the targets into making a mistake that leads to compromise.

The presentation will cover the attack methodology (including sanitized emails and web pages), the results, modifications considered for future attacks, and recommendations to make an ICS and individuals less susceptible to this focused social engineering attack.

3:00 – 4:15                      Application Whitelisting in Two Parts

Part I – Application Whitelisting for Industrial Control Systems - An Evaluation Guideline  
Sebastian Obermeier, Ragnar Schierholz & Hadel Hadel of ABB Corp Research Switzerland

Several whitelisting solutions were evaluated for use in ICS. The evaluation method and the conducted test results, which range from the exploitation of windows vulnerabilities to the execution of files via alternate data streams, will be presented. The authors will point out some identified limitations and bugs of whitelisting products in an anonymized form, and show the difficulties for vendors when it comes to the evaluation of the quality of such software.

Important questions will also be addressed such as the “update process question” and the “anti-virus question”.

DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



Part II - No Silver Bullets: Application Whitelisting in ICS  
Andrew Ginter, Waterfall Security

Application whitelisting is emerging as an essential component of new "best practice" cybersecurity programs for industrial control systems. Some whitelisting vendors have claimed their technology can "prevent all unauthorized change, including all malware". This is inaccurate. This paper demonstrates how whitelisting technologies are blind to memory-based attacks, scripted attacks and misuse of existing, approved executables. The attacks are demonstrated on a major control-system whitelisting technology. While whitelisting may be essential to the emerging best practice, we need to be aware of the limits of the technology in order to position it correctly within comprehensive security programs.

4:15 – 4:30                      Faking Out Security Enumeration Tools  
Bryan Owen, OSISOft

This brief presentation looks at methods to provide false information back to common scanners such as nmap and Nessus. It also asks the audience if this is worth doing.

4:30 – 5:15                      Correlating Process Events with Security Events to Detect Attacks  
Eric Knapp, NitroSecurity

The PI server and other ICS historians collect large amounts of process data. Security Information and Event Management (SIEM) products collect security events and correlate them detect cyber attacks. This presentation looks at how process data collected in a historian can be presented to a historian and used to enhance attack detection. Specific deployment examples with real world data will be presented as well as ideas to enhance this approach.

5:15 – 7:30                      5<sup>th</sup> Annual S4 Cocktail Party





DAY 2:

8:30 – 10:30 Project Basecamp: Hacking and Exploiting PLC's

Research Team: Dale Peterson and Reid Wightman, Digital Bond  
Independent Researchers Dillon Beresford, Jacob Kitchel, Ruben Santamarta and two anonymous researchers

The Siemens S7 vulnerabilities have highlighted a PLC that is both insecure by design and has exploitable vulnerabilities. While this has not been a surprise, few PLC's have undergone this much public scrutiny.

Project Basecamp is an effort by a team of researchers to hack and exploit seven different PLC's/field devices. These are very popular devices widely used in the critical infrastructure.

The researchers agreed to test eight different attack categories and then were free to use their creativity to expand testing beyond that. The two-part presentation will analyze the results and look for common failings and areas where certain field devices are more secure than others. Successful attack methodologies will be described, specific examples will be covered in detail and demonstrated, and examples of automating the attacks in exploit frameworks will be shown.

Part I: PLC Attack Methodologies and Analysis of Overall Results

Part II: Specific PLC Attacks and Exploit Examples

10:45 – 11:15 Denial of Surface?  
Eireann Leverett  
Advisors: Dr. Frank Stajano, Prof. Jon Crowcroft of Cambridge Univ.

Are ICS devices that are insecure by design exposed on the Internet? The author has located more than 10,000 Internet accessible, ICS-related devices globally – including HVAC systems, building management systems, meters, PLCs, RTUs, and other industrial control devices using data that covers a two year time window. The results were processed using a prototype tool that leveraged various data sources to find exposed systems, visualize them on a map based on IP geo-location, provide a timeline view of events, and present details of potentially applicable exploits. Our intention is to use such a tool to visualize and prioritize the remediation and security perimeter improvement of such devices in a risk-based manner.



The author has also begun working with ICS-CERT and other organizations (who chose to remain anonymous) to inform asset owners of their exposure. Part of the presentation will contain the experience of working on exposure remediation at a global scale, and the experience of collaborating with ICS-CERT and others to bring greater awareness of such exposure.

11:15 – 12:00      Preventing Attacks on Critical Infrastructure through Hardware Protection Against Malicious USB Devices  
Pascal Sitbon, Arnaud Tarrago, Pierre Nguyen of Electricite de France

Recent attacks on ICS, like the famous Stuxnet, use USB slots to penetrate into physically isolated networks. In this paper, we propose a new way to protect those entry points while enabling at the same time their use for authorized purposes like Human-Machine Interface (keyboard, mouse, etc.). This approach is based on hardware-level security with selective control and access to USB peripherals. A prototype device will be presented as well as real-case examples highlighting the security value for Critical Infrastructure's operators.

The presentation and prototype will cover requirements such as protection against unauthorized devices; protection against inappropriate behavior of authorized devices; protection independent of the level of security of the computer itself; and security embedded in electronic components that aren't re-programmable.

12:00 – 1:00      Lunch on the patio overlooking the intercoastal waterway

1:00 – 1:15      Unsolicited Response

1:15 – 1:45      Intrusion Detection for Embedded Control Systems  
Jason Reeves, Ashwin Ramaswamy, Michael Locasto, Sergey Bratus,  
and Sean Smith of Dartmouth College

As a large number of embedded systems are deployed as part of the smart grid rollout, securing these devices becomes a top priority. On top of the usual resource constraints of an embedded device, however, embedded power SCADA systems impose additional constraints that make the "standard" approach to intrusion detection-using virtualization in some manner-infeasible of these devices. In contrast, we suggest taking an in-kernel approach to intrusion detection, and demonstrate that a program operating inside of (and at the same privilege level as) the OS kernel is a viable way to protected embedded power systems.

In this talk, we detail the Autoscopy Jr. system built in a Dartmouth College lab, which



leverages the built-in tracing framework of an operating system to monitor it for control-flow anomalies indicative of rootkit behavior. Additionally, Autoscopy Jr. also features a profiler program that allows us to customize our monitoring scope to balance the security and performance needs of the host. In tests on a standard desktop system, our system imposed a post-profiling overhead of 5% or less on a wide range of performance benchmarks. We will also discuss our work in using Autoscopy with two specialized kernels (one with an optimized probing framework, and another with a hardening patch installed), and the issues we encountered therein.

1:45 – 2:00                      Lessons Learned From Certifying Embedded Devices  
Graham Speake, Yokogawa

The ISA Security Compliance Institute (ISCI) has an Embedded Device Security Assurance Certification. PLC's and other devices have both successfully achieved certification and failed one or more of the required tests. This brief session will highlight some of the areas where vendors have had most difficulty in meeting the certification requirement and potential ways vendors can better meet these requirements.

2:30 – 3:30                      The Great Debate: Anti-virus and Monthly Security Patching Should Be  
Abandoned in ICS

The Great Debate format has been very popular in past S4 events. One attendee is selected and given ten minutes to make the best possible case for the proposition. Another attendee makes the best case against the proposition. Then it is a free flowing debate amongst all attendees with a vote at the end determining the winning side.

3:00 – 3:15                      Break

3:15 – 4:00                      Live Forensics in Control Systems  
Dr Bradley Schatz, Queensland University of Technology, Brisbane

Current efforts towards securing the control systems focus on preventative security and detection measures, however operational constraints are often in conflict with such measures. In such an environment the requirement for an enhanced responsive capability is significant; however, there is currently an absence of methodologies and tools supporting live forensic incident response in this environment.

DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



This paper will summarize the results of a yearlong collaborative project within the Australian electricity sector, focused on enabling post attack live forensic investigations with minimal impact to operations. The researchers had access to a recently decommissioned (1 month prior) control system, with simulated (replayed) field device traffic beyond the FEP. The project was very much about identifying the general applicability of live IT forensic techniques in this environment, and gave some interesting results regarding the risks of particular acquisition approaches to availability.

4:00 – 4:30	To Be Announced – A Placeholder for the Inevitable Surprise Topic in ICS Security Prior To S4
4:30 – 4:45	Closing Remarks

DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



## CONFERENCE LOCATION

S4 is held at the Florida International University (FIU) Kovens Conference Center. This is a beautiful facility, and ideally suited for interaction of 60 top ICS security researchers. The sessions will be held in a small auditorium / case study room designed for interaction.



Lunch and the cocktail party will be served outside on the terrace overlooking the intercoastal waterway in the beautiful South Florida weather. Transportation will be provided from the conference hotel to the Kovens Center.



SECURING THE CRITICAL INFRASTRUCTURE

DIGITAL BOND'S

# SCADA SECURITY SCIENTIFIC SYMPOSIUM



## CONFERENCE HOTEL

The official S4 hotel is at the Marenas Resort, a new, beautiful hotel right on the beach. It is a short ride to the FIU conference center (transportation will be provided). It is also a short ride to the infamous South Beach scene. We will send details on how to book the hotel after you register for S4. The price is a real bargain for Miami Beach in January. A large, 700 square foot suite with kitchen and private balcony right on the beach is \$229/night. The best Internet price for this room is \$459/night.

The hotel has a good restaurant, nice bar for post conference discussions, a large spa and exercise room and many other amenities. Many attendees bring family down to enjoy Miami Beach in January at a luxury resort.

Reserve your room at [www.marenasresortmiami.com](http://www.marenasresortmiami.com). Click on Additional Reservation Options, then Group on this new page, and use group code 48890 through December 15th. Or call and make your reservation at 877.858.2305.



There are additional hotels nearby that are off the beach and slightly less expensive.

- Courtyard By Marriott (Aventura)
- Hampton Inn (Hallandale)