An Invitation To Participate In

The 2006 SCADA Security Summit: Deciding What Works in Securing Distributed Control Systems in the Critical Infrastructure

If you are a critical infrastructure asset owner who uses SCADA, PLC or DCS systems, or a control system technology or security developer or researcher, we hope you will join us in Orlando, FL, March 2-3, 2006 for the first SCADA Security Summit. The Summit is the next step in implementing the Roadmap to Secure Control Systems initiative being modeled by the energy sector. The Summit brings together significant stakeholders in a collaborative development workshop to identify the subset of security technologies and processes that measurably improve security of control systems.

The Summit is a gathering of the **technical experts** in the organizations that operate and secure the critical infrastructure of the United States, Great Britain, Canada, New Zealand, and Australia (called asset owners in this document). Asset owners include private and governmental organizations responsible for gas and oil production and distribution, electricity production and transmission/distribution, water and sewer systems, railroads, chemical plants, and other industries that use SCADA (Supervisory Control and Data Acquisition) or DCS/PCS Distributed Control Systems / Process Control Systems solutions/equipment to administer critical automation systems in their organizations.

Goals Of The Summit

There are two primary goals of the Summit. One is to identify effective technical solutions for SCADA security. The other goal is to initiate processes that will convert those "promising practices" into procurement specifications, and maintenance requirements for control systems asset owners to use when evaluating and purchasing new control system technology or security technology for control systems, and when negotiating continuation of maintenance contracts for existing control systems. Summit participants will actively use their technical knowledge and experience in facilitated work group sessions. Control System security issues will be framed and awareness will be provided through brief level-setting topic area presentations that will introduce each work group session.

The Summit has two specific purposes:

1. to enable the asset owners of the critical infrastructure to jointly determine "what works." They will identify the technologies, products, processes, and controls that have proven themselves effective or can do so very quickly and can be implemented in the short and intermediate term to reduce the exposure of SCADA systems to cyber attack through electronic means, and
2. to develop procurement language that the operators can use to ensure the SCADA systems they are buying or maintaining have the best available security.

Very Different From Traditional Conferences

The Summit is different from traditional conferences in five important aspects:

1. The conference is about action, not talk. Asset owners in the audience will actually vote on technologies for further testing and immediate implementation priority.

2. Long discussions about which standards are better than others and presentations about the theory of effective security in control systems are completely excluded.
3. Vendors cannot "buy speaking slots" by spending a lot of money on exhibits.
4. The solutions being discussed will be vetted for effectiveness before they are selected for inclusion.
5. The action continues after the conference as the most promising technologies are fully proven and common procurement specifications are prepared.

Participation In The Summit

There are two ways to participate in the summit:
1. As a representative of an asset owner.
2. As a representative of an organization that can offer solutions that improve SCADA security.

The Summit is open to all. Asset owner representatives may register by visiting www.sans.org/registration/register.php?conferenceid=1278. Asset owners who have implemented security processes that work may submit proposals to give brief summaries of their promising practices in a special session that will highlight their discoveries. Instructions for submitting proposals are below.
All other participants will be allowed to participate by invitation only. Invitations are being extended to representatives of four groups (called security solution providers) to meet with and address the asset owners and operators to help them meet those goals:
1. Suppliers of SCADA, DCS or PLC systems who have made significant advances in securing their systems.
2. Suppliers of communications and security devices and software who have developed products that can significantly reduce the threat of electronic attack against current industrial automation systems.
3. Research leaders who have discovered technologies or processes that can significantly reduce the threat of electronic attack against current industrial automation systems.
4. Standards organizations that are developing standards that, when implemented, can be shown to significantly reduce the threat of electronic attack against current industrial automation systems.

The Agenda: Before, During, And After The Summit

Prior to the Summit, the organizing committee will solicit and review suggestions of solutions from solution providers (vendors, researchers, standards experts) to whom invitations will be extended to address the Summit. The format for these suggestions (proposals) is formally defined in order to allow a fair competition among them. The Organizing committee will select the speakers. Proposals are due by December 10, 2005. Selections will be completed by January 10, 2006.
The Summit will consist of a series of facilitated panel sessions in which the invited solution providers (suppliers, researchers, and standards experts) will give short presentations of the technologies or other solutions they propose for near- or intermediate-term deployment. Each panel will also have discussants who will respond to the proposed solutions and ask the panelists specific questions to uncover the strengths in their proposed solutions. The audience will also be given the opportunity to ask questions. At the end of each session, the participating asset owners will be asked to make preliminary ratings of the proposed solutions, based on

what they heard, so that the program organizers can identify a short list of the most promising technologies and processes for reducing the electronic threat to SCADA systems.
Over a period of weeks following the Summit, the organizing committee, working with the selected solution providers, will create a set of proposed procurement language that asset owners and operators can use if they so choose to ensure the SCADA and DCS products they buy and use have the most effective security possible.

2006 SCADA Security Summit: Conference Committee

Leadership Groups

- Hun Kim and Andy Purdy, National Cyber Security Division, US Department of Homeland Security
- Karl Williams, UK National Infrastructure Security Co-ordination Centre
- Hank Kenchington, Office of Electricity Delivery and Energy Reliability, US Department of Energy
- *Alan Paller, The SANS Institute

Asset Owners

- *James Cupps, BP
- *Ian Henderson, BP
- *Will Pelgrin, Chief Information Security Officer, State of New York and Chairman of the Multi-State ISAC
- Andrew Hildick-Smith, Massachusetts Water Resources Authority (MWRA)
- Tom Flowers, Center Point
- Tom Good, DuPont Co
- Evan Hand, Kraft Foods Inc.
- Seiki Harada, BC Hydro Canada
- Jay White, Chevron Texaco
- Tom Bowe, PJM
- Stuart Brindley, Independent Electricity System Operator, Ontario, Canada

Research Groups

- *Mike Assante, Idaho National Laboratory
- Jennifer DePoy, Sandia National Laboratory
- Eric Byres, British Columbia Institute of Technology
- George Cybenko, Dartmouth University, I3P
- Andrew Wright, Cisco Critical Infrastructure Assurance Group

Standards, Government and Industry Groups

- Mike Torppey, cal Director, Process Control Systems Forum
- Bill Rush, Gas Technology Institute
- Tom Kropp, EPRI (Electric Power Research Institute)
- Tom Donahue, Information Operations Center, US Central Intelligence Agency

- Gerald S. Freese, AEP

** Organizing Committee Co-Chairs*

2006 SCADA Security Summit: Speaker Submission Requirements And Topics

Proposal Submissions Requirements

Your proposal submittal MUST include:

1. Identifying information including the submission author's name, title, organization, address, email, telephone, and FAX numbers, and similar information about any co-authors.
2. A description of the security threat your solution addresses, the types of asset owners and SCADA or DCS systems to which it applies.
3. The solution, including details of how it works. If the proposed solution can not be expected to be implemented (at least in a real-world pilot test) in the next six months, explain what is left to be done to reach that stage. If your solution is based on commercial hardware or software tools, name them.
4. Data on the solution's effectiveness: before and after comparisons, evaluations, direct savings, trade-offs, etc. This is important. It needs to answer the question, "How do you know this works?" It would be great if it can also answer the question "How do you know it doesn't introduce additional vulnerabilities of performance problems?"
5. Lessons learned.
6. A 5-7 line summary of your talk that we can place in the brochure.

How to submit your proposal

You may submit a Text file or Word Document. If available a sample presentation file in PowerPoint would also be helpful to the organizing committee. Email it to scadasecurity@sans.org no later than 5 PM EDT December 10, 2005. Earlier submissions will be reviewed first so prompt submission will improve your chances to be invited. Once the proposals are narrowed down to a small group, the submitters may be asked to provide more details.

Possible Topics For the SCADA Security Summit

1. A secure core architecture including secure control/communication protocols
2. Identity management, authorization, authentication and role/location based access control
3. Intrusion detection and prevention systems (both network and host-based)
4. Cryptographic protection for network traffic to and from PCS/SCADA
5. Intelligent firewalls/interfaces/filters between the PCS/SCADA and enterprise networks
6. Practical and effective solutions for securing wireless networks connected to SCADA/control system networks
7. Practical and effective techniques for blocking viruses and spyware
8. Practical and effective patch management, node enumeration and alerting, and configuration and change management
9. Seamless authentication and authorization of operators, technicians, partners,

vendors.

10. Defenses against denial of service attacks
11. Wide-area secure administration for very large or geographically dispersed SCADA/Control System sites

This is a living document. To propose other topic sets, email scadasummit@sans.org. List the topic, suggested solutions to be included under the topic, and explain how you know implementing those solutions over the next 12 months will lead to immediate and measurable reductions in the threat from cyber attacks.