



SMART GRID
Cyber Security

Conference & Expo
August 10-11, 2010
San Jose, CA

Web Site

Home Register Who Should Attend Venue Conference Program Speakers Sponsors Knowledge Partners

Conference Program Thursday, August 12, 2010 Register Login

REGISTER TODAY!

[Get Email Updates >>](#)

Text/HTML

Day One
Program at a Glance -- August 10, 2010

7:00 am

Registration Opens –

Badge Pickup, Networking and Continental Breakfast

9:00 am

Opening Remarks:

Data security is only as strong as the weakest link -- while more endpoints and more interconnected networks mean more ways for security problems to get in and proliferate. Solving the problem is the challenge, and this is what the conference is focused on: strategies, challenges, needs and technologies. Hear from the Conference Chairman about the objective of this Summit and the areas covered in this inaugural event.

Mike Ahmadi, COO & Vice President, GraniteKey, Conference Director

9:15 am

Keynote Address:

What is the Value of Smart Grid Security?

Most experts find it hard to make a case for the value of smart grid security, even though they are convinced it's very important. Fortunately, this problem is more tractable than it appears. One part of the solution is to understand exactly how the smart grid would create value on a day to day basis. The surprise here is how big the gains can be—if all the components of the new system can be made to work together harmoniously. Another part of the solution is to understand the way in which the smart grid contributes to the creation of additional value over the long term by increasing the grid's resilience. This contribution can be partially quantified by assessing the degree to which the rest of the economy is affected by a loss of electric power and how this changes with the length of an outage. (The result is very different from what's been claimed in the media!) Once there is sufficient clarity about the value created by the smart grid, it becomes possible to estimate the value that could be destroyed by various types of attacks on it. The resulting assessments may only indicate ranges of magnitude. But they will still be accurate enough to show why smart grid security needs to be a top priority!

Scott Borg, Director and Chief Economist, US Cyber Consequences Unit

9:45 am

Research: Key Findings on the Emerging Smart Grid Cyber Security Market

A high level perspective of the market drivers, key players, and evolution of marketplace for secure systems, components and services emerging for smart grid deployments.

Bob Gohn, Senior Analyst, Pike Research

10:15 am

Panel: Best Practices in Grid Detection and Prevention

This panel bring together cyber security thought leaders to share insight and perspective on the actual threat to grid security today; what the threat scenario may be over the next 1 to three years. Also, learn more about best practices in cyber security prevention that have emerged in this early stage of grid deployment.

Mark Schaeffer, CEO, GraniteKey LLC

Gib Sorebo, AVP/Chief Cybersecurity Technologist, SAIC

Matthew Carpenter, Senior Security Analyst, InGuardians

David Baker, Director of Services, IOActive

11:15 am

Networking Break

11:30 am

Keynote Address:

Commissioner Philip Moeller, Federal Energy Regulatory Commission

12:00 pm

Hosted Lunch Break

1:00 pm

Security and Vulnerability of Control Systems

Performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak. This makes some

control systems and control system networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. In fact there have already been a number control system cyber incidents. This session will discuss some of the unique issues with control systems, what can be done to secure them, and what shouldn't be done.

Joe Weiss, Applied Control Solutions, LLC

1:30 pm

How Public Carriers Enable End to End Secure Connectivity for AMI /AMR and HAN Applications

All Smart Grid applications require secure wireless connectivity, as well as an effective and proven partner to ensure encryption and system integrity. This session focuses on how Verizon delivers wireless security for Utility and non-utility data collection models being deployed today.

Sowmya Varadarajan, Distinguished Member of Technical Staff, Verizon Wireless

2:00 pm

ROUNDTABLE: Assessing Last Mile Architecture as a Security Vulnerability
Moderator: Stephen McGrath, Director of the WCA (Wireless Communications Alliance)

Rob Conant, Senior Vice President, Networks, Trilliant

Sowmya Varadarajan, Distinguished Member of Technical Staff, Verizon Wireless

2:45 pm

Securing the Edge of the Grid

Devices that exist at the edge of the Smart Grid are typically small and resource-constrained. They include smart meters, SCADA devices and sensors, which are distributed throughout generation, transmission and distribution networks. Securing these new nodes at the edge is a highly complex endeavor. At the same time, a lot of the current security discussion has been focused on singular aspects such as the threat from foreign nation-states. However, taking a comprehensive approach to security at the edge of the Smart Grid appears to be better. This session aims to discuss three aspects of Smart Grid security for end-nodes: encryption and decryption on small devices, a user-friendly approach to scalable key management and technology requirements that allow for reliable device authentication.

Chris Hanebeck, Vice President Product Marketing and Management, Reverse Security

3:15 pm

Networking Break

3:30 pm

Managing the Cyber Security Threat

Understanding the psychology of security and the layers of concern with regard to smart grid security, physical layer, privacy layer and cyber layer.

Ernest Hayden, Managing Principal - Senior Energy Security Consultant, Verizon Business – Global Energy & Utility Vertical

4:00 pm

NERC Requirements on Smart Grid Infrastructure

NERC regulatory standards, while needed, have posed a significant challenge to the power industry over the past few years. Various approaches to NERC compliance have been used as each utility struggles to manage or contain the risk of noncompliance, while the standards themselves have evolved and deadlines have passed. Where does a Smart Grid infrastructure play into all of this? Rob Shein will discuss the implications of current NERC requirements on different aspects of Smart Grid infrastructure, as well as some of the current evolutions that will shape future requirements, as well as describe some approaches that can reduce the risk.

Robert Shein, Security Architect, Enterprise Services, Energy Practices, HP

4:30 pm

Round-table Session: The Perspective and Path Forward – the Energy Utilities

Leading executives offer a candid and informal discussion from their perspective of the threat to physical infrastructure, customer data, the solutions being offered and the cost/benefit for undergoing a review of security vulnerability and assessment.

Moderator: Andy Bochman, Energy Lead, IBM

Bobby Brown, Director of Communication & Information Systems Security, Enernex

Chris Peters, Vice President, Critical Infrastructure Protection, Entergy
Mike Echols, Security Principal, Salt River Project

5:30 pm

Hosted Reception

Day Two

Program at a Glance -- August 11, 2010

7:00 am

Registration Opens

Badge Pickup, Networking and Continental Breakfast

9:00 am

Opening Remarks:

Mike Ahmadi, COO and Vice President, GraniteKey LLC, Conference

Chairman

9:10am

Keynote Address:

Dr. Cohen will provide an overview of the challenges and solutions associated with protecting the emerging smart grid. Starting with the unique consequences associated with smart grid technologies, the problems driving the present situation will be identified from a standpoint of management decision-making. The lack of good information, combined with inadequate expertise available and applied, and inadequate decision-making leads to a situation that will take more time to fix than the present approach to the smart grid allows. The key question is not whether we will proceed with smart grids, but how we will overcome these critical challenges. And this is the question this talk will answer.

Fred Cohen, President, [California Sciences Institute](#)

9:45 am

Roundtable Session: The Vendors -- Security Technologies and Components

This roundtable features executives from technology firms supplying critical components of the smart grid. Understand the current state of leading vendors' accomplishments in baking security into their current products.

Stephen Chasko, Principal Security Engineer, Landis & Gyr

Robert Former, Principal Security Engineer – R & D, Itron

Edward Beroset, Director of Technology & Standards, Elster Solutions Inc.

Stan Chan, Director of Strategic Initiatives, Verisign

10:45 am

Networking Break

11:15 am

Intelligent Cyber Security Techniques and Strategies for 21st Century Smart Grid

Dr. Emmanuel Hooper, General Dynamics IT , Division of Security and Systems Assurance, Federal Energy Regulatory Commission

11:45 am

Bringing PKI Based Solutions To The Smart Grid - A Practical Approach To Authentication, Identity and Supply Chain Management

Experts in enterprise IT, e-commerce, banking, and Internet services know that PKI-based technology provides the strongest and most effective authentication solution available today. PKI-based solutions are effective at managing identity as well as controlling the supply chain of secure components. The rapidly growing (and huge) global embedded devices market has struggled with adopting PKI-based solutions due to technical, logistical, and cost barriers. The session discusses how recent innovations now allow PKI-based security to be cost effective and deployable in embedded system products requiring a strong authentication technology.

Nadaradjane Ramatchandiran, Senior Business Development Manager, Renesas Electronics America Inc.

12:30 pm

Lunch Break

1:15 pm

The Trend in MicroGrids Deployment and Implementing Security at the Campus Level

One of the most promising trends in energy: Microgrids, smaller-scale electrical systems spanning college campuses, municipalities and business parks, where energy is generated, stored and very closely managed on an intensely local level. Understand the challenges to cybersecurity in the second wave of smart grid deployment: microgrids.

Christine Hertzog, Consultant and Author, Smart Grid Library

Eve Schooler, Principal Engineer, Intel Labs, Energy Systems Research

Kurt Yeager, Executive Director of the Galvin Electricity Initiative

Alan McDonnell, President of Non-Synchronous Energy Electronics, Inc.

Isaac Ghansah, Ph.D., Professor of Computer Science and Computer

Engineering; Director, Center for Information Assurance and Security, California State University Sacramento

2:15 pm

Roundtable: State of the Threat -- Proven Flaws or a Theoretical Challenge or a Media Sensation?

The conference concludes with a wide ranging discussion on the state of the smart grid cyber security threat. Take part in the discussion to gain a consensus about the true nature of the national threat – a proven flaw in the architecture of the smart grid or a fear-driven marketing and media environment.

Andy Bochman, Energy Security Lead, IBM

Elinor Mills, Senior Writer, CNET

David Scott Lewis, Author/network blogger & "Letter from China" columnist at NanoEnergy Report & AlwaysOn Network and Sand Hill Group

3:00 pm

Conference Concludes

Copyright 2010 by Interwork Media Inc.

[Terms Of Use](#) [Privacy Statement](#)