NRC Fuel Cycle Facility Cyber Threat Conference

May 30, 2013

8:30am to 5:00pm

The Center for Advanced
Engineering Research (CAER),
1173 Research Park Blvd, Forest, VA 24551

CLOSED MEETING DUE TO SENSITIVE, CYBER SECURITY-RELATED DISCUSSION PLANNED

AGENDA

8:30am—8:40am	Welcome Brian Smith, Branch Chief Uranium Enrichment Branch NRC Office of Nuclear Material Safety and Safeguards
8:40am—9:00am	Opening Remarks Cathy Haney, Director NRC Office of Nuclear Material Safety and Safeguards
9:00am—9:45am	Cyber Security and the Advanced Persistent Threat Mike Shinn, NRC Cyber Security Specialist (Ctr.)
9:45am—10:00am	Break
10:00am—10:45am	Cyber Security and Industrial Control Systems Tim Shaw, NRC Cyber Security Specialist (Ctr.)
10:45am—11:30am	Expert Panel Q&A Tim Shaw, NRC (Moderator) Mike Shinn, NRC Mario Fernandez, NRC Dr. Carl Elks, University of Virginia Jonathan Chugg, Idaho National Laboratory Kenneth Rohde, Idaho National Laboratory Jeff Morgan, FBI
11:30am—1:00pm	Lunch Breakout Session (Starting at 12:30pm) Security Considerations for Portable and Mobile Devices
1:00pm—4:30pm	Technical Demonstrations (Rotations, 1 Hour Each) Firewall Technologies (Group A) - Considerations for use of firewall technologies as boundary control devices. Industrial Control Technologies (Group B) - Demonstration of known ICS cyber attack methods. Safety System Technologies (Group C) - Overview of common weaknesses in safety system design.
4:30pm—5:00pm	Closing Remarks

DEMONSTRATION ROTATIONS

Time	*Group*	*Demo*	*Room*
1:00 to 2:00 pm	A	Firewall Technologies: Consideration for use of firewall technologies as boundary control devices	Classroom
	B	Industrial Control Technologies: Demonstration of known ICS cyber attack methods	Conference Room
	C	Safety System Technologies: Overview of common weaknesses in safety system design	ICS 6B
2:10 to 3:10 pm	A	Safety System Technologies: Overview of common weaknesses in safety system design	ICS 6B
	B	Firewall Technologies: Consideration for use of firewall technologies as boundary control devices	Classroom
	C	Industrial Control Technologies: Demonstration of known ICS cyber attack methods	Conference Room
3:20 to 4:20 pm	A	Industrial Control Technologies: Demonstration of known ICS cyber attack methods	Conference Room
	B	Safety System Technologies: Overview of common weaknesses in safety system design	ICS 6B
	C	Firewall Technologies: Consideration for use of firewall technologies as boundary control devices	Classroom
4:30 pm – 5:00 pm	All Groups	Closing Remarks	Control Room

NOTES

BIOGRAPHIES

Mr. Jonathan Chugg is a member of the Cyber Security Research and Development Department at the Idaho National Laboratory in Idaho Falls, Idaho. Mr. Chugg is part of the SCADA and Control Systems security research team primarily focused on identifying and mitigating vulnerabilities in computer systems responsible for the Nation's critical infrastructure. He is also is an active member of the INL Cyber Security Red Team. Mr. Chugg received his Bachelor's Degree in Computer Science from Idaho State University in 2005.

Dr. Carl Elks is currently with the School of Engineering and Applied Science at the University of Virginia. Dr. Elks received his M.S. and Ph.D. from the University of Virginia. Prior to joining the University of Virginia, Dr. Elks worked for NASA Langley Research Center for 10 years conducting research on advanced fault-tolerant fly by wire control systems, and automated flight deck systems. His research interests are in the analysis and design of application critical embedded systems and their infrastructures, which are typically found in such areas as nuclear power generation, advanced main control rooms, wireless control, and SCADA systems. He is the co-founder of the Center for Safe and Secure Nuclear Energy in Lynchburg, Virginia.

Mr. Mario Fernandez is a Cyber Security Specialist assigned to the Reactor Security Oversight Branch, Division of Security Operations, in the NRC Office of Nuclear Security and Incident Response. Since joining the NRC, Mr. Fernandez has been responsible for developing various programs in the areas of physical and cyber security which include physical security training, cyber assessment team activities, cyber security inspection training for NRC inspectors, and the NRC's cyber security oversight program. Prior to joining the NRC, Mr. Fernandez worked at Calvert Cliffs Nuclear Power Plant for 10 ½ years in the Security Department.

Mr. Jeff Morgan is an Industrial Control Systems Analyst for the Federal Bureau of Investigation (FBI). He holds a degree in Information Management from the Marriott School of Business at Brigham Young University and has 22 years' experience in information and telecommunication systems design, installation, maintenance, and management in the Healthcare and Transportation industries. His troubleshooting philosophy is "If your second idea doesn't work either, follow the wire."

Mr. Kenneth Rohde is a member of the Cyber Security Research and Development Department at the Idaho National Laboratory in Idaho Falls, Idaho. Mr. Rohde is part of the SCADA and Control Systems security research team primarily focused on identifying and mitigating vulnerabilities in computer systems responsible for the Nation's critical infrastructure. He has served as Adjunct Faculty with the University of Idaho Computer Science Department and also been a guest lecturer at the Idaho State University. Mr. Rohde received his Bachelor's Degree in Computer Science from the University of New Mexico in 2000.

Mr. William "Tim" Shaw is a Cyber Security Architect for MAR, Incorporated and cyber analyst for the NRC where he specializes in the development of technical guidance, regulatory oversight activities, and support of NRC Cyber Security Roadmap regulatory initiatives. He is a Certified Information Systems Security Professional (CISSP) and has been active in industrial automation for more than 30 years. He is the author of Computer Control of BATCH Processes and Cyber Security for SCADA Systems. Shaw is a prolific writer of papers and articles on a wide range of technical topics and has also contributed to several other books.

Mr. Michael Shinn is the President of Prometheus Global with over 20 years of professional experience in business and security operations, governance programs, and technology development, with sub-specialties in risk management, regulatory affairs, security services and technology validation. He formerly worked for Cisco Systems as a research scientist, and the White House as a computer security and forensics analyst. He serves as a cyber security specialist for the NRC, is the co-author of several federal publications, and technical contributor to NRC Regulatory Guide 5.71, "Cyber Security Programs For Nuclear Facilities" and various regulatory reports associated with cyber security in the nuclear sector.