

Users Speak, I

Users Define Requirements for Manufacturers
– Authentication, Authorization, Access
Control, Encryption

John E. Allen

Ernst & Young
(602) 625-2044

john.allen@ey.com

Today's Objectives

- Provide a forum for users to identify what is needed from control systems vendors
- Organized around types of technologies useful to provide or improve control system security (based on technology types in TR99.00.01)

Discussion Topics this morning

- **Authentication and Authorization Technologies**
Role based, password, challenge/response, physical/token, smart cards, biometrics, location based, device to device, and password management and distribution
- **Filtering, Blocking and Access Control Technologies – firewalls, VLANs, etc.**
 - [A SCADA-Aware Distributed Firewall - Eric J. Byres, Darren Lissimore and Khai Lee - Group for Advanced Information Technology, BCIT](#)
- **Encryption – symmetric key encryption, public key encryption and key distribution, private key signatures and digital certificates, and VPN**
 - [Understanding TKIP; the Latest Ethernet Security - Jim Weikert, ProSoft Technology, Incorporated](#)
 - [Cyber security tools for SCADA, Dennis Holstein](#)
 - [\(Short\) Cyber security tools – Architecture Overview – Dennis Holstein](#)

Future vision ideas

- Give me every control system object such that:
 - Security functions are integrated and seamless
 - Every object can be secure and includes all these attributes, as routinely as controllers include setpoint, gain, and reset rate
 - Security is already a key design criteria that I don't need to add later
 - Security can be configured by the user
 - "Strong" security is enabled by default

Future vision ideas, continued

- Multiple security technologies are built in every object, to provide defense in depth to the level required by the user's configuration
 - Authentication and authorization can be required to send another object data or to use another object's data or to communicate with humans
 - All object's are capable of "strong" filtering, blocking, and access control for all communications with other network objects and humans
 - Any object's communications with other objects can be encrypted outside of it's physical boundaries (from transmitters to HMIs – any device on the control network)
 - All object's physical boundaries provide physical security or awareness of physical security
 - All objects provide for audit, measurement, monitoring, and detection



Discussion